WORKING
PAPER

Assessing the Benefits of Homeland Security Efforts Deployed Against a Dynamic Terrorist Threat

BRIAN A. JACKSON

WR-465-DHS

February 2007

INFRASTRUCTURE, SAFETY, AND ENVIRONMENT

Assessing the Benefits of Homeland Security Efforts Deployed Against a Dynamic Terrorist Threat

Brian A. Jackson[1]
Associate Director, Homeland Security Program
RAND Corporation

Given the diversity of the roles and missions of the Department of Homeland Security and other government organizations involved in protecting the United States, homeland security policies are intended to provide a wide variety of societal benefits.[2] A discussion of the benefits of homeland security policies could therefore reach from the everyday benefits produced by smooth movement of goods and services across the nation's borders to how polices address exceptional situations like major natural disasters. However, because the management of risk – particularly the risk associated with terrorism – is such a central part of DHS' mission, how to assess the benefits of policies aimed at protecting the nation from terrorist attack is a primary focus in this area of policy analysis and debate.

In efforts to address the risks posed by terrorism, principal homeland security activities include detecting and characterizing threats and their consequences; attempting to reduce the chance of risk exposure through deterrence; limiting the potential for terrorist risks to affect society through hardening or other mitigation activities; putting response and recovery assets in place to address the consequences of risk exposures when they occur; and investigating after terrorist attacks to identify and apprehend the perpetrators. To do these, homeland security efforts bring together a variety of technological tools, manpower, and other resources into a national defensive effort. These homeland security activities complement other national strategies designed to limit the threat of

[1] This discussion is based on the findings of a research effort sponsored by the Department of Homeland Security, Science and Technology Directorate, Office of Comparative Studies that focused on defensive technologies, though the arguments can be applied to measures aimed at combating terrorism more broadly (see, Jackson, et al., *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, MG-481-DHS, Santa Monica, Calif.: RAND Corporation, 2007). The views expressed are the author's and do not necessarily represent those of RAND or any of its research sponsors.

[2] Due to the many federal, state, and local organizations involved in the implementation of measures aimed at protecting the nation from a range of risks, this paper will use the term homeland security measures or efforts broadly, reaching beyond the sole and specific activities of the Department of Homeland Security.

terrorism including activities aimed at reducing the desire of individuals and groups to cause harm (e.g., shaping intent through communications efforts, diplomacy, and other approaches) and offensive actions aimed at taking on groups directly (e.g., military operations or the actions taken by intelligence organizations abroad.)

These security, preparedness, anti- or counter-terrorism measures (referred to collectively here as measures to combat terrorism) may either target the terrorist group itself, e.g., information gathering activities aimed at identifying and apprehending group members or disrupting the group's finances, or seek to defeat or blunt terrorist attempts to stage attacks on desirable targets, e.g., measures intended to allow disruption of an operation, responses to limit its effects once the attack has been initiated, or measures to reduce its consequences (and, as a result, its ability to produce damage and fear) after the it has occurred (Figure 1).

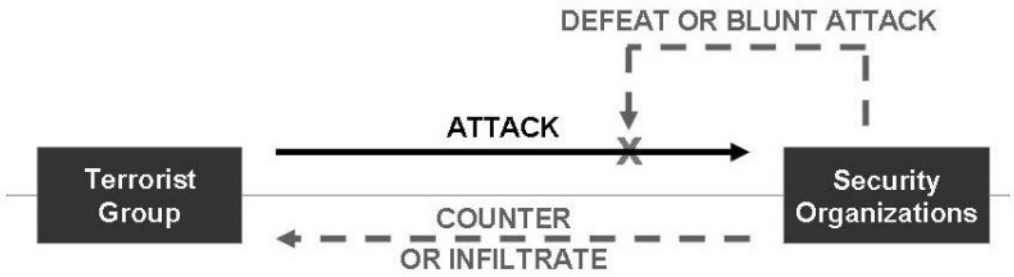

Figure 1 – Two Classes of Measures to Combat Terrorism

Though research over many years has produced a deep academic and policy literature on many questions associated with terrorism and counterterrorism, one that remains largely unanswered is how to measure the benefits produced by activities aimed at addressing terrorism risk. From the perspective of security organizations, what is important is how protective and security actions affect what a terrorist group can do – whether it can stage fewer attacks, whether it is denied the use of damaging weapons, and whether when it stages attacks they are less damaging or more likely to fail. Each of these changes could reduce the costs terrorists can impose on society and, therefore, justify the investment of public monies in protective measures. That reduction in costs involves components that can be readily considered in monetary terms (damages avoided) and components where

explicit values are more difficult to estimate (value of maintaining citizen feelings of safety and confidence).

With the formation of DHS and the significant expenditures that have been made on homeland security measures since 2001, there is increasing interest in analytical methods for measuring or estimating what particular policies produce so their benefits can be compared to their costs. This type of information is critical to ensure the nation is getting the most risk reduction for its investment and so homeland security policies can be improved over time. Actually making quantitative estimates of such benefits is challenging, requiring both estimates of expected attacks and their consequences as well as the effect particular measures on terrorist capabilities and is the focus of increasing analytical efforts. Understanding appropriate ways for doing so – in spite of an unpredictable threat whose consequences are difficult to forecast – is the focus of expanding policy and analytic effort.

Terrorist Adaptation as a Threat to the Benefits of Security and Protective Measures

One characteristic of terrorism that makes assessing the benefits of security and protective measures particularly challenging is the fact that terrorist groups represent an adaptive rather than a static threat. Unlike risk management or protective actions taken against many risks – e.g., the hazard presented by an environmental pollutant – a terrorist group has both the incentive and frequently the ability to change itself as a direct response to deployed protective measures. Actions targeted at a terrorist group may threaten its very existence. For those aimed at constraining its offensive activities, the organization's effectiveness and its freedom to act to advance its agenda are at stake.

Terrorist adaptation in response to security and preparedness measures (shown in Figure 2) can target either the security measures aimed at defeating or blunting terrorist attacks (e.g., a group seeking ways around defenses) or actions taken against the group directly (e.g., developing improved operational security measures to avoid surveillance or infiltration). If terrorist counter-efforts are successful, the value of protective or security measures will be significantly reduced. A circumvented defense will not reduce the

group's ability to stage attacks and countered surveillance will provide no information to guide arrest or prosecution of group members.

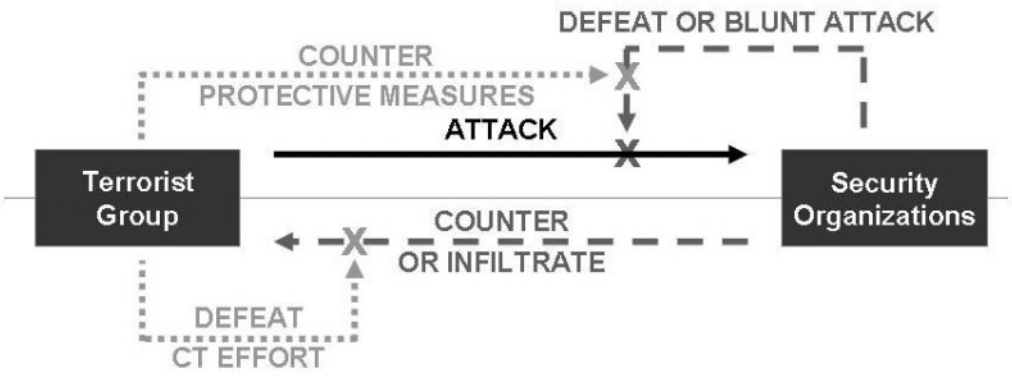

Figure 2 – Terrorist Counter-Efforts to Defensive Measures

In considering the effect of terrorist counter-efforts on the benefits of security measures, it is useful to shift from thinking about the benefits of homeland security as the costs it *prevents* terrorists from imposing on society and instead view them as measures that *impose* costs or risk on terrorist adversaries. Security actions aimed at a terrorist organization impose costs and risks directly – the personal risk of capture and incarceration (or physical harm) to group members, and the loss to the organization of the services of key personnel. Actions aimed at defeating or blunting terrorists' attack operations impose operational costs and risks (as well as potentially direct risk to individuals involved in an attack) by either reducing the utility of available attack modes or potentially causing attack operations to fail. In both cases the intent of protective and security measures is to either deter adversaries from staging attacks or significantly degrade their ability to cause harm when they choose to do so.

Focusing on the costs security measures impose on the terrorist group is, admittedly, a significant simplification. For determining the value of expenditures on security, it is the costs they prevent terrorists from imposing that are indeed most important – and the costs they impose on the adversary are only a means to achieving that prevention. Depending on the sensitivity of a particular adversary to the costs defenses impose, how those costs "translate" to changes in terrorist behavior could differ considerably. Furthermore, this

approach ignores all benefits from such measures that are not directly linked to terrorism, for example, against other risks like natural disaster or non-terrorist sabotage. Doing so is nonetheless useful since it simplifies discussion by focusing on the components of this problem most relevant for considering terrorist behavioral change and adaptation and, for the remainder of this discussion, we will use those costs as an (albeit partial) proxy for the benefits of security and defensive measures.

Terrorist Adaptation in Response to Defensive Measures

Understanding how terrorist organizations respond to the introduction of security measures is hampered by the availability of complete and detailed data. In contrast to terrorist attacks, events that are almost by definition overt and detectable, adaptive behaviors in response to defenses are frequently covert and, therefore, difficult to compile extensive datasets for analysis. To examine this behavior, RAND carried out a set of case studies of terrorist responses to defensive measures.[3] The research team selected for study terrorist organizations that were comparatively sophisticated and had operated over a long duration (suggesting that they were capable of responding to defensive action) in conflict with similarly sophisticated states (suggesting a variety of defensive measures would have been deployed against the groups.) The organizations examined were the Provisional Irish Republican Army; the Liberation Tigers of Tamil Eelam; Jemaah Islamiyah and its affiliates; and Palestinian groups operating against Israel. The studies were based on information collected from published literature and other public data sources, as well as in-person interviews with members of government organizations engaged in fighting the selected groups.

Across these groups, a common set of four counter-defensive strategies was identified:

- Altering operational practices – By changing the way they operate or manage themselves, groups blunted the effectiveness or concealed themselves from defensive measures. For example, in response to the deployment of surveillance

[3] Reported in Jackson, et al., *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, MG-481-DHS, Santa Monica, Calif.: RAND Corporation, *forthcoming*

systems, groups shifted their travel and communications modes to render the monitoring ineffective.

- Changing or replacing technologies used by the terrorist group – By acquiring new technical tools or changing existing ones, groups sought to limit the impact defenses had on their effectiveness. For example, in response to the use of jamming to prevent use of remote detonators for bombs, groups shifted the frequencies they used or adopted new detonation modes.

- Avoiding the defensive measures – In cases where doing so was possible, some groups simply moved away from areas covered by defensive measures to avoid their effects. Examples included shifting from defended targets to sites not protected by defenses or moving operational areas to ones where defenses had not been deployed.

- Attacking the defenses directly – In some cases, groups that were limited by defenses simply broke through them by attacking the defenses themselves. For example, multiple or larger bombs were used to overwhelm hardening or other protections around targets. In some cases, "attacks" on defenses involved subverting them for the terrorists' purposes, such as using detection or other systems to trigger behavior by security services that made them vulnerable to attack.

While categorizing terrorists' counter-defensive strategies provides a way to structure discussion of many unique adaptive behaviors, it should be noted that these categories are not mutually exclusive and do overlap to some extent. Furthermore, to defeat a particular defense, some terrorist efforts utilized multiple strategies. These four general strategies therefore represent a palette of options groups might draw on in an attempt to reduce the costs defensive measures imposed on them. Within each category, specific counter strategies ranged from actions that were essentially costless for groups to implement (e.g., small alternations in behavior to confuse an intelligence gathering system) to those

that might be quite costly (e.g., replacing its arsenal when a defensive measure rendered current weapons obsolete).

Describing the Effect of Terrorist Adaptation on the Stream of Benefits Provided by Security Measures Over Time

To understand the effects of terrorist adaptation on the value of homeland security measures, it is necessary to think about those measures as imposing a *stream* of costs on an adversary over time, rather than a single value measured at one point in time. Security and preparedness measures do not produce one benefit when they are introduced, rather they *begin* to deliver their benefits at that point. This transition from a static to a dynamic perspective is illustrated in the notional graphs shown in Figure 3.[4]

The single X on the y-axis of the notional graph at the left illustrates the purely static view – a single measurement of the costs imposed on adversaries at one point in time. Viewed from a dynamic perspective, the effect of a security measure is not just one cost, imposed once on an adversary, but is instead a stream of costs imposed on adversaries during each time period in which the security measure is deployed.

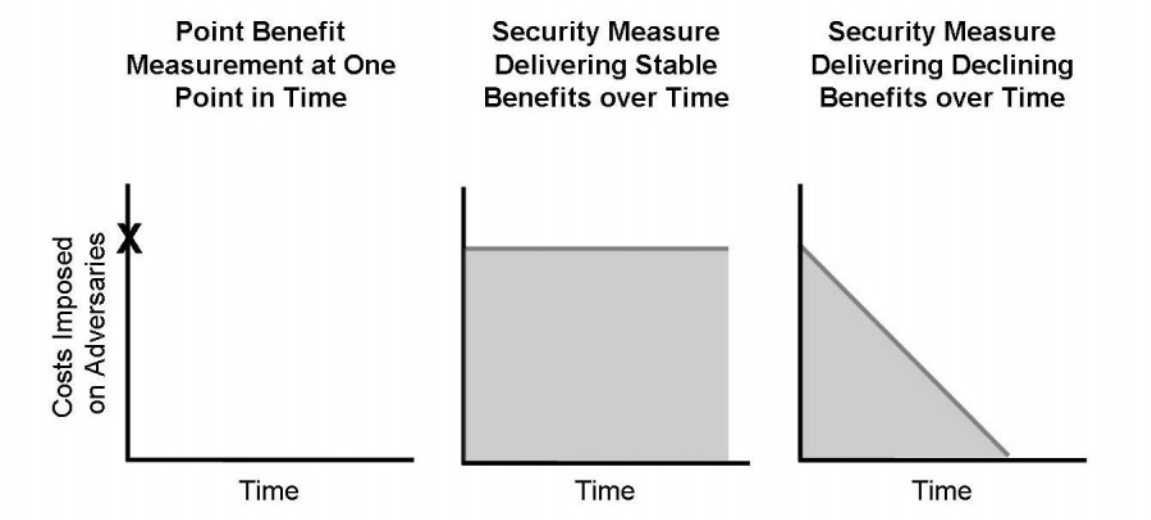

Figure 3 – Static versus Dynamic Views of Security Measures' Benefits

[4] It should be noted that viewing benefits in this manner is in no way unique to the assessment of security and preparedness measures. Such a transition from a static to a dynamic perspective is needed for fully understanding any cost or benefit stream with the potential to change over time as circumstances change.

Viewed this way, the value of a security measure (the sum of the stream of costs it imposes on adversaries between the measure's introduction and the present) is the area under the curve defined by measurements each period it has been deployed. For a security measure that delivers a constant benefit that area is rectangular (the shaded area in the center graph); for measures whose benefits decline over time (whether due to terrorist adaptation or a variety of other potential causes), the benefit stream will define a different, perhaps more complicated area (e.g., the triangle in the rightmost graph).

In practice the effect of specific terrorist behavioral or other change on security performance is likely to be quite complex. Responding to defenses placed around a particular set of targets could involve a number of strategies drawn from the listing above. Adaptive strategies differ in effectiveness, and implementing some would require the group pay additional costs to do so.[5] For large and geographically dispersed groups, different elements of the terrorist organization might respond differently, leading to changes that might offset each other when total benefits are considered. However, for the purposes of discussion, it is useful to break down the effects of terrorist reactions into a few exemplary categories and generalize about their overall effect on the benefits provided by security and protective measures.

[5] It should also be noted that the choices made by adversaries about how they adapt to defenses may have broader effects on the levels of terrorism risk to a nation than we have considered here. In this discussion, we have limited ourselves to examining the benefits of defenses as the costs they impose on the terrorist group, rather than the damages they prevent a group from inflicting. From that perspective, a group moving to the use of vehicle bombs to overwhelm defenses rather than using small explosive devices would still produce a benefit stream because the logistical burden on the group would be higher as a result. However, moving from small bombs to very large ones is a significant escalation in the level of violence and could increase the casualties and damages associated with each terrorist operation. This escalation in the potential outcomes of attacks could outweigh any benefit that the costs impose on the group. As a result, even successful defenses (i.e., those that impose costs on a group) could produce changes in behavior that increase total terrorism risk. The need to consider the broader shaping effect of defenses on terrorist behavior and how it might affect terrorism risk is discussed further in the report on which this discussion is based (Jackson, et al., *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, MG-481-DHS, Santa Monica, Calif.: RAND Corporation, *forthcoming*). This emphasizes that a complete understanding of the value of defenses must look both at the costs imposed from the attackers point of view (as in this discussion) and how the defenses and subsequent changes may alter the costs the attacker can impose (which is not covered in this discussion.)

I. Terrorists Costlessly "Break the Code" of the Defense, Rendering it Obsolete

In some cases and for some defensive measures, terrorists may be able to discover a way to circumvent a defense at little or no cost. Such a situation is analogous to a group discovering a secret that allows it to "break the code" of the defense – e.g., identifying how a particular type of intelligence is collected and what is necessary to make it impossible to do so. The effect of such a situation on the benefit provided by a security measure is straightforward to describe: assuming the change can be implemented by the terrorist organization quickly, the resulting benefit graph would look like that shown in Figure 4A. If the change takes time to implement throughout the terrorist organization, the drop-off in benefits might occur more gradually over time, but would eventually reach zero when all terrorist cells possessed the required information or capability to evade the defense. As suggested by the graph reaching zero, for this case it is assumed that implementing the countermeasure to the defense does not cost the terrorist group anything (beyond, perhaps, modest costs at the point where the countermeasure is implemented).

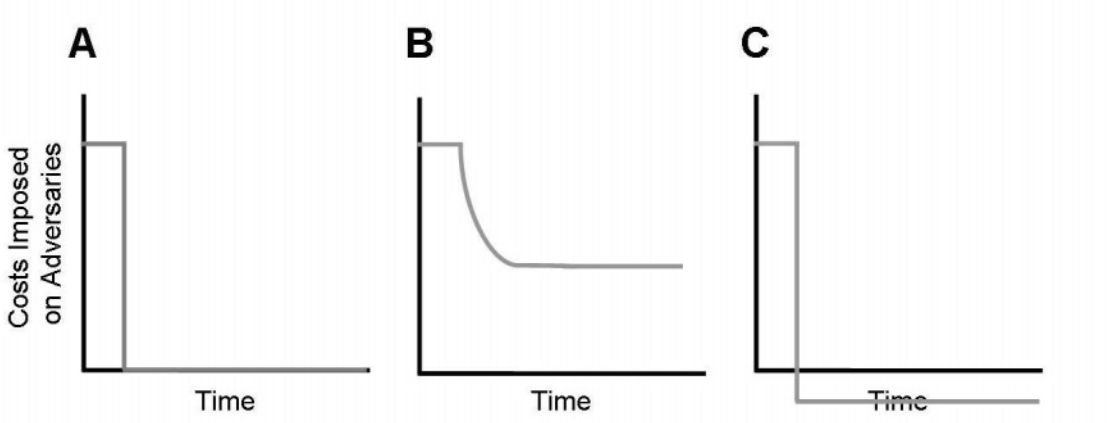

Figure 4 – Illustration of the Effects of Terrorist Adaptation on the Benefits of Security and Protective Measures

II. Terrorists Defeat the Defense, but Must "Pay" to Do So

Even if the terrorists find an answer to a defensive measure, if there is a price associated with implementing the countermeasure, the defense may still impose some costs on the group. This could result in a benefit stream like the one illustrated in Figure 4B, where

even though the group might have neutralized the defense, doing so requires the group to pay other costs. For example, a group may be able to shield itself from a new intelligence gathering method, but only by constantly spending time or resources to do so. Alternatively, a group may find ways to continue to attack a particular target with the same effectiveness that it could before the defense was introduced, but can only do so through the use of much more expensive weaponry or tactics (where expensive could be viewed in terms of monetary, time, personnel, or other group resources).

In these circumstances, the defensive measure may appear to be failing to have any effect – i.e., the group still appears able to what it did before – yet the costs imposed by the defensive measure should not be discounted since they are forcing the consumption of resources that could be used for other purposes.

III. Terrorists Adapt and Degrade – But Not Eliminate – the Functioning of the Defense

In many cases, it will not possible be for the terrorist to completely eliminate the costs a defensive measure imposes, only to reduce them from their intended level. Such attenuation of defenses would also produce a benefit stream like that shown in Figure 4B, where the costs imposed on the adversary drops from its initial value, but never reach zero. Such a situation could arise because a group is simply unable to change sufficiently to fully eliminate the effect of the defense. For example, a group might be able to continue to attack a protected target with its current weaponry, but – because the weapon is less effective because of the defenses – those attacks will be at a reduced level of effectiveness. As a result, rather than providing complete protection, the defense instead mitigates some terrorist risk at the target.

IV. Terrorists Turn the Security Measure Against the Defense

Rather than simply seeking to defeat a defensive measure, in some cases terrorist groups can learn how to use security or protective systems in ways that serve their own interests rather than those of the nation deploying them (Figure 4C). The clearest examples of such circumstances are found for detection or information gathering systems. Detectors can be used to cause false alarms, producing response costs as well as undermining trust

in the functionality of the system itself. Calls to terrorism "tip lines" can similarly be used to manipulate defenders, where the responses to false calls are used to bring citizens or members of security organizations into harms way.

In Figure 4C, a case is illustrated where not only does a group costlessly neutralize a defensive system (taking its benefits to zero), but then uses it against the defense (moving the cost line into negative territory.) This represents an extreme case for the purposes of illustration where the complete compromise of the defense converts it from an asset to a liability. In other situations, efforts to turn a security measure against defenders could result in a situation more akin to Figure 4B, where this provides a way for the terrorist to degrade, though not eliminate the value of the defense.

Risk Displacement – Adding a Spatial Dimension

In the previous discussion of the effect of terrorist adaptation on security benefits, the focus has been on only one dimension, the variation of total benefits of a defense over time caused by adaptation in terrorist operational practices, technological behaviors, avoidance, or attacking defenses directly. For these concepts to be expanded and applied to benefits assessment under realistic circumstances, variation over other dimensions would have to be addressed as well. In particular, the ability of terrorists to use the third adaptive strategy described above – moving their operations or activities in an effort to avoid a defensive measure – could have an effect on the spatial distribution of security benefits even if total benefits remained the same.

Just as the benefits of security measures can be viewed as a stream accruing over time, they can also be viewed spatially as separate streams accruing in different places. Broadly acting defensive measures (e.g., strong border control) produce benefits by making it more difficult to attack many targets simultaneously, while localized defenses (e.g., barriers around a single target) may produce benefits in only one place. Terrorists can respond to localized defenses by simply moving elsewhere. As a result, while a defense may appear to be functioning effectively in the area where it is deployed (producing a benefit stream like the solid rectangle in Figure 3), if it has only moved the risk elsewhere it may not be producing a net regional or national benefit.

The Risk of "Adaptive Destruction" of Security Measures and Assessing the Design of Homeland Security Efforts

To accurately assess the benefits homeland security measures deliver once they are deployed and in service, the potential effect of terrorist adaptation and counter-defensive efforts must be addressed. Doing such assessments in a static way, e.g., as a single measurement when a technology is first deployed, is inappropriate given that nature of the threat can change considerably over time. If policymakers assume that defensive measures provide a stable benefit in spite of adaptation by adversaries, we may significantly overestimate their value and the protection they provide. If adversaries continue to adapt, the divergence between assumed protection and reality may increase significantly over time. Understanding the impact of these terrorist behaviors is particularly important for defensive measures with significant operations and maintenance costs, since such on-going expenditures may only be justified if the defense continues to provide some minimum level of effectiveness.

Beyond its relevance for measuring the benefits of deployed security measures, the risk that terrorists will circumvent security measures – "adaptive destruction" of the benefits they deliver, even if they are not destroyed themselves – suggests two other lessons relevant for assessing different technologies and technology programs while they are still in their design phases. They are:

- Consider whether defensive measures can be modified to respond to changes in terrorist behavior – If the design of a defensive measure locks it in to a single configuration or operating mode, its benefits are vulnerable to changes in terrorist behavior. If the security measure is static,[6] it will not be able to adjust to a dynamic threat. In contrast, if flexibility is built into the defense from the start – e.g., when a terrorist group "breaks the code" to its functioning, it is possible to

[6] Depending on the security measure, the technological characteristics – e.g., the nature of a detection technology – could make it difficult or impossible to change in response to adaptation by an adversary. In other situations, it is the combination of technology and the way it is used – e.g., including the concept of operations, etc. – where changes in how the technology is applied could make it possible to respond to countermeasures.

change the code and reconstitute performance – then options exist to preserve the benefit stream provided by the defensive measure (Figure 5A). Including this type of robustness against dynamic threats in evaluation of potential defenses is important, since providing it may require additional expenditures up front when the defense is designed and implemented. If it is not considered, options that could provide robustness may be inadvertently sacrificed in an effort to reduce costs.

- Assess the potential benefits of portfolios of defensive measures, rather than single defenses in isolation – Given the reasonable desire to ensure deployed defenses are effective, there is frequently a focus on designing individual security measures to deliver as high a level of protection as possible. When facing an adaptive adversary, however, a strategy where resources have been focused on developing and optimizing single defensive measures are risky (Figure 5B), since the benefit of the entire security effort could drop to zero if the defense is breached. This is one reason behind the idea of defense in depth – maintaining multiple lines of protection against high risk threats – to maintain some protection even if some defenses are breached.

  Even if multiple defensive lines are not all deployed at the same time, a portfolio approach to development of defensive measures could provide "fall back" options if an initial defense becomes obsolete. Depending on the level of adaptive threat, multiple sub-optimal defenses (Figure 5C) may actually provide a larger total benefit than one highly effective option. To explicitly recognize the value of having options available to reestablish protection in the event the first line defenses fail, evaluation of defensive efforts cannot focus exclusively on individual security measures in isolation. Evaluation of programs of defensive development – and the *portfolios* of options the programs are building to address particular defensive needs – is necessary to capture this element of terrorist risk.

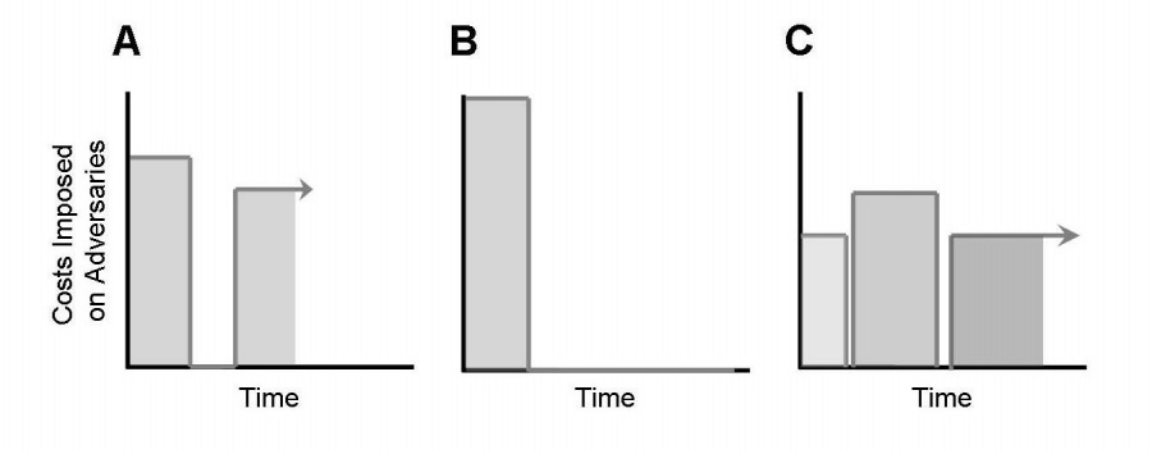

Figure 5 – Illustration of the Benefit Streams Produced by Different Defensive Design Approaches

Conclusions

In contrast to many risks government policy makers seek to manage, the risks posed by terrorist organizations must be viewed from a dynamic rather than a static perspective. When challenged by defenses that limit their operational effectiveness or threaten them, violent groups will change their behavior to reconstitute their capabilities and security. Such adaptation represents a significant risk to the benefit stream provided by security technologies. Protective measures may deliver their expected performance when they are introduced, but simply assuming that they will always deliver stable performance could create a false sense of security. Like technical, schedule, and budget risks, this risk of "adaptive destruction" by adversaries must be addressed in program management if protective benefits are to be sustained over time, and included in assessments of homeland security measures to ensure all necessary information is available for policy and program decisions.