Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **2009**	2. REPORT TYPE	3. DATES COVERED **00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE **Understanding Why Terrorist Operations Succeed or Fail**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Rand Corporation,1776 Main Street,PO Box 2138,Santa Monica,CA,90407-2138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**41**	

This product is part of the RAND Corporation occasional paper series. RAND occasional papers may include an informed perspective on a timely policy issue, a discussion of new research methodologies, essays, a paper presented at a conference, a conference summary, or a summary of work in progress. All RAND occasional papers undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

OCCASIONAL
PAPER

Understanding Why Terrorist Operations Succeed or Fail

Brian A. Jackson, David R. Frelinger

RAND HOMELAND SECURITY PROGRAM

Project supported by a RAND Investment in People and Ideas

This Occasional Paper results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by the generosity of RAND's donors and by the fees earned on client-funded research.

Library of Congress Cataloging-in-Publication Data

Jackson, Brian A.
Understanding why terrorist operations succeed or fail / Brian A. Jackson, David R. Frelinger.
p. cm.
Includes bibliographical references.
ISBN 978-0-8330-4767-0 (pbk. : alk. paper)
1. Terrorism—Psychological aspects. 2. Terrorists—Attitudes. 3. Terrorism—Planning.
4. Terrorism—Prevention. I. Frelinger, Dave. II. Title.

HV6431.J2838 2009
363.325—dc22

2009029748

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published 2009 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

Created in the wake of the September 11, 2001, terrorist attacks, the Department of Homeland Security came into being with the daunting core mission of taking action to protect the nation from terrorist attack and the simultaneous requirement to continue to perform the numerous other critical functions of all its component agencies. The complexity of the department's mission was further compounded by the fact that it depended not only on the success of the department's component agencies, but also on the efforts of a national homeland-security enterprise comprised of organizations at the federal, state, and local levels, both inside and outside government. That there have been challenges in carrying out this endeavor in the years since should surprise no one. However, it has also been the fortunate reality that, whatever those challenges, at the time of this writing, there have been no major terrorist attacks within the United States since 9/11.

This paper is one of a series of short papers that began as the result of a RAND research effort during the transition in presidential administrations in 2008–2009. As the first change in administration since the creation of the Department of Homeland Security, this period represented an opportunity to reexamine and revisit the goals of homeland security policy and assess how we as a nation are trying to achieve them, ask whether what we are doing is working, and make adjustments where necessary. The goal of RAND's research effort was not to comprehensively cover homeland security writ large, but rather to focus on a small set of policy areas, produce essays exploring different approaches to various policy problems, and frame key questions that need to be answered if homeland security policy is to be improved going forward. The results of this effort were diverse, ranging from thought experiments about ways to reframe individual policy problems to more wide-ranging examinations of broader policy regimes. These discussions should be of interest to homeland security policymakers at the federal, state, and local levels and to members of the public interested in homeland security and counterterrorism.

This paper examines the issue of why terrorist operations succeed or fail. Given the importance of this issue for security planning, there is a significant literature on the topic, and a variety of these contributions identify factors that can shape operations going well or poorly. This paper reacts to and responds to that literature and proposes an overarching framework for thinking through why attack options can have very different outcomes. In it, we argue that such a framework is critical for security planning efforts because focusing on individual factors in isolation risks producing an overall picture that does not accurately describe terrorist behavior.

This effort is built on a broad foundation of RAND homeland security research and analysis carried out both before and since the founding of the Department of Homeland Security. Examples of those studies include:

- Brian A. Jackson, Peter Chalk, Kim Cragin, Bruce Newsome, John V. Parachini, William Rosenau, Erin M. Simpson, Melanie W. Sisson, and Donald Temple, *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, Santa Monica, Calif.: RAND Corporation, MG-481-DHS, 2007.
- Tom LaTourrette, David R. Howell, David E. Mosher, and John MacDonald, *Reducing Terrorism Risk at Shopping Centers: An Analysis of Potential Security Options*, Santa Monica, Calif.: RAND Corporation, TR-401, 2006.
- Henry H. Willis, Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby, *Estimating Terrorism Risk*, Santa Monica, Calif.: RAND Corporation, MG-388-RC, 2005.

Although the ideas and frameworks described in this paper have been developed over several years of research for the Department of Homeland Security, the National Institute of Justice, the Defense Threat Reduction Agency, the Office of the Secretary of Defense, and other sponsors, the views expressed herein are not necessarily those of RAND or of any of its research sponsors. The authors would also like to acknowledge the contribution of the two reviewers of the manuscript, Bruce Hoffman and Ami Pedahzur, whose comments were very helpful in improving the paper. Its remaining shortcomings are the sole responsibility of the authors.

The RAND Homeland Security Program

This research was conducted under the auspices of the Homeland Security Program within RAND Infrastructure, Safety, and Environment (ISE). The mission of RAND Infrastructure, Safety, and Environment is to improve the development, operation, use, and protection of society's essential physical assets and natural resources and to enhance the related social assets of safety and security of individuals in transit and in their workplaces and communities. Homeland Security Program research supports the Department of Homeland Security and other agencies charged with preventing and mitigating the effects of terrorist activity within U.S. borders. Projects address critical infrastructure protection, emergency management, terrorism risk management, border control, first responders and preparedness, domestic threat assessments, domestic intelligence, and workforce and training. Information about the Homeland Security Program is available online (http://www.rand.org/ise/security/). Inquiries about homeland security research projects should be sent to the following address:

Andrew Morral, Director
Homeland Security Program, ISE
RAND Corporation
1200 South Hayes Street
Arlington, VA 22202-5050
703-413-1100, x5119
Andrew_Morral@rand.org

This Occasional Paper results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by the generosity of RAND's donors and by the fees earned on client-funded research.

Contents

Figure

Summary

Understanding why terrorist attacks succeed and fail is important for homeland security and counterterrorism planning. In examining past terrorist attacks, this understanding is necessary to discern why attackers sometimes are very successful and why sometimes even reasonably well-planned operations fall apart. Discerning ways to make attacks less likely to succeed is a central goal of efforts ranging from homeland security technology development to the direct military engagement of terrorist groups. Given the importance of the issue, many analysts have approached the problem from a variety of different directions. Success and failure in the context of terrorist attacks have been defined in different ways, from the strategic down to the tactical level. Many factors that make contributions to operations going well or poorly have been identified.

But in our work focusing on security planning, we have found the results of many of these past analytic efforts difficult to apply. In part, this is because of the tactical focus of such planning, but it is also because of the absence of a unifying framework that brings together the range of factors that can influence the success and failure of terrorist operations in a practical and applicable way. Based on past research examining a variety of terrorist groups and security planning problems, we have developed just such a unifying framework. At the heart of our model lies our contention that the past success or failure of a terrorist operation—or the likelihood that a future attack will succeed—can be best understood by thinking about the match or mismatch between three key sets of characteristics:

- terrorist group capabilities and resources
- the requirements of the operation it attempted or is planning to attempt
- the relevance and reliability of security countermeasures.

For a terrorist attack to have the greatest chance of success, there needs to be (1) a match between its capabilities and resources and the operational requirements of the attack it is seeking to carry out and (2) a mismatch of security countermeasures and intelligence/investigative efforts with both the group and its plans.

Previous studies of why terrorist operations may succeed or fail include a variety of specific examples of factors that fall into each of these three classes, but in considering how such factors shape the outcomes of attacks, we argue that analysis and threat assessment should focus on the match or mismatch between factors rather than on the factors themselves:

- First, organizing thinking in this manner gets beyond analyzing factors in isolation to focus on key relationships, and in many cases, it is the nature of the relationship—rather than the absolute values of any of the factors—that truly contributes to a terrorist attack going as its authors planned. This is important for developing accurate threat assessment because focusing on the factors rather than relationships could lead to either artificially high or low assessments of the threat posed by a group.

- Second, focusing on these sets of matches and mismatches provides a more systematic way of thinking about how different classes of security measures align or do not align to different types of threats. The search for certain mismatches between protective measures and possible attack operations is traditional vulnerability-based threat assessment, but combining thinking about how a specific attack team might or might not overmatch a guard force of known capability with how well passive measures do or do not match those same threats provides a more integrated approach to protective planning.

  Similarly, looking at how security efforts either do or do not align with groups of varied characteristics is a different way of thinking about surveillance or intelligence planning. While being prepared to capitalize on group operational security mistakes is important, considering how changes in security measures might create new matches that benefit the defense is a more proactive strategy. For example, if changes in the security around a high-profile target sufficiently increase the operational security requirements for pre-attack surveillance, that mismatch may mean future attackers will be forced to attack without enough information to stage a consequential operation.

- Third, identifying mismatches between a group's capabilities and what is known about its intentions may also provide clues to security organizations as to what activities to watch for in the future. A significant mismatch (if it has been recognized by the group) would suggest the need for more pre-attack preparation on the terrorists' part to reduce the shortfall, potentially creating additional opportunities to detect and disrupt their activities. The more a group stays within its comfort zone and only seeks to stage operations that are well within its capabilities, the less pre-attack preparation would likely be required and the quicker it could stage operations; therefore, there would likely be fewer opportunities for intervention.

  In these potential differences among groups—between groups seeking to carry out operations well within their capabilities versus those that are reaching beyond what they can currently achieve—we see as an additional reason to draw a distinction between characteristics (e.g., a group's operational skills) and the processes that can affect them when considering why operations succeed and fail. Beyond just avoiding the potential for double counting during an analysis of why an operation might succeed or fail, mixing the two could result in intelligence efforts missing an opportunity (e.g., recognizing the need for particular types of training by a group and therefore focusing attention on detecting it) or underestimating the threat posed by a group that has not been observed carrying out a process that it does not, in fact, need to stage successful future attacks.

These strengths lead us to conclude that focusing attention on a small set of practical relationships in this manner—how different characteristics do or do not match one another—could help to guide analysis of why past terrorist operations went as they did, and, more importantly, could help to identify opportunities to shape the chance of success or failure of future operations.

Understanding Why Terrorist Operations Succeed or Fail

Examining the history of terrorism, it is relatively straightforward to find examples of brutally successful terrorist operations that went exactly as the groups involved planned. It is similarly straightforward to identify attacks that did not go at all like their perpetrators thought they would. For some operations, the attackers' goals—and the fact that they achieved them—are obvious; for example, assassinations of individual leaders in which a bullet or explosive is delivered with deadly accuracy and precision. Conversely, there are many examples of operations that broke down either in part or in total: bombing attacks in which bombs did not detonate; attacks that missed their intended target, sometimes striking people even the terrorists themselves would have preferred not to kill or injure; assassins who killed the wrong person; plots months or years in the making discovered and disrupted by police; attackers on route to a target stopped in their tracks by alert guard forces; and the list goes on.

Understanding what separates successful from failed terrorist actions is clearly important for security planning. As a result, a variety of previous research efforts have sought to identify factors that shape why some operations go as planned and others break down (for example, Drake, 1998; Hoffman, 1985; Oots, 1986; Sandler and Scott, 1987; Sharif, 1996; and most recently, Homeland Security Institute, 2007). In this paper, we react and respond to this literature and build on it by proposing an overall framework for thinking through the range of individual factors and various drivers of the outcomes of terrorist operations and for considering their implications for planning.

In some unsuccessful or partially successful terrorist operations, the attackers involved are the authors of their own misfortunes—shortcomings in skills or preparation make their chances of successfully executing their plans slim at best. As with any individual or organization, when terrorists' reach exceeds their grasp, they will most likely fall short of their objectives. In other failed terrorist acts, the actions of security organizations are responsible for detecting and derailing their plans. In still others, factors beyond the terrorists' control defeated their efforts. As is the case for any disparate group of organizations attempting to achieve similar goals, success and failure rates differ: There are hardened and professional organizations that routinely achieve their operational objectives, while more-amateur terrorist groups only get lucky occasionally.

An understanding of why attacks succeed or fail can make a range of contributions to security planning:

- If there are ways that counterterrorism and security measures can increase the chances that operations *will* fail, then identifying those opportunities can increase the effectiveness of security plans.

- Given the many ways that groups could stage attacks, a clear understanding of why some attacks succeed and others fail can help prioritize security efforts. Tactics and attack types that are more likely to fail on their own may merit less security investment than other attacks.
- A clear understanding of why attacks go well or poorly can contribute to the post-hoc assessment of terrorist operations, enabling these efforts to more clearly assess the strengths and weaknesses of security efforts.
- Such an understanding is also useful for assessing future threats—and identifying which of them are of most concern. Though "failure of imagination" has been cited as a reason why emerging terrorist threats have not been anticipated, there are dangers associated with "excessive imagination" as well. Unconstrained brainstorming can always "conjure up more diabolical scenarios than any security system can protect against" (Jenkins, 2001). Understanding which among these "diabolical scenarios" are more likely to fail can let planners focus on eliminating the attack modes that give attackers the most leverage.[1]

The success and failure of terrorist groups has received substantial analytical attention. Some studies have sought to understand success and failure at the strategic level and how, from the terrorists' perspective, campaigns of attacks or particular actions did or did not contribute to achieving the terrorists' goals. Recent examples of analyses at this level include studies of the efficacy of suicide bombing campaigns (e.g., Pape, 2003; Moghadam, 2006; Atran, 2006) and overall analyses of terrorism as a strategy (e.g., Abrams, 2006; Kydd and Walter, 2006). Tactical level analyses focus on the details of specific operations and define success based on what happened during and after an attack (e.g., Pedahzur et al., 2003; Sharif, 1996; Ahmed, 1998; Oots, 1986; Sandler and Scott, 1987; Benmelech and Berrebi, n.d.), and many analysts look for correlations between attack outcomes and group characteristics. More-structured efforts to identify factors related to the success or failure of individual operations have combined case studies with this type of data analysis (e.g., Homeland Security Institute, 2007). Previous work at RAND has examined different types of terrorist operations (as well as other small-unit military and paramilitary operations) in search of factors that shape whether individual operations will or will not succeed (e.g., Vick, 1995; Meyer et al., 1993; Hoffman, 1985; Jenkins, 1981).

Definitions of what *success* and *failure* in the context of terrorist operations differ across the literature. Some either implicitly or explicitly view success and failure in a binary fashion, judging an attack successful if it occurred regardless of its specific outcome (e.g., Pedahzur et al., 2003). Others have used more-complex definitions of terrorist success, including that *the operation was logistically complete* (e.g., the weapon was delivered to the target and it went off) and other factors such as *the operatives involved escaped unscathed* (e.g., Sharif, 1996). Some analysts make the assumption that attackers are seeking to maximize certain operational effects (e.g., causalities),[2] and they assess the success of operations either in relation to the theoretical maximum number of those effects the operation could have been expected to produce under

[1] Another of the papers in this series addresses this topic specifically (Jackson and Frelinger, 2009).

[2] In recent years, the focus has been on al Qaeda as an organization that made maximizing causalities a central goal, but some earlier terrorist thinkers expressed similar views: In his essay "Murder," published in 1849, Karl Heinzen wrote "that the greatest benefactor of mankind will be he who makes it possible for a few men to wipe out thousands. . . . [our enemies have] left us no other choice than to devote ourselves to the study of murder and refine the art of killing *to the highest possible degree*" (Heinzen, 1849, emphasis added).

ideal conditions (e.g., Kaplan and Kress, 2005; Wein and Liu, 2005)[3] or by where a specific operation falls in the output distribution of other similar operations (e.g., Benmelech and Berrebi, n.d.). There are also challenges in deciding whether success and failure should be assessed explicitly from the perspective of the terrorists planning the attacks (i.e., did they achieve what *they* intended)[4] or from the perspective of the nations targeted by terrorism or the security organizations that oppose them.

In our view, although such previous efforts have wrestled with the question of why individual operations may succeed or fail, a comprehensive picture is still lacking. This absence makes it difficult to apply the results of past analytical efforts to security planning. This is in part because of the varying constructions of success and failure in the literature. While none of the ways success and failure have been framed is incorrect, the use of each to analyze security and counterterrorism can lead to different analytical outcomes. Moreover, in our view, an additional key element required to pull together past results into a comprehensive picture is missing: a clear framework for assessing how the many variables and factors that might correlate with or affect the outcomes of terrorist operations relate to and influence one another. Based on our past work, those relationships and interactions appear to be more important than the variables and factors themselves.

In this paper, we propose a framework for thinking about terrorist operations' success and failure that is focused at the tactical level, a framework in which success and failure is defined by (1) whether a terrorist operation occurs (i.e., is not disrupted by police or security organizations) and (2) its outputs in causalities, damage, and other effects directly related to the way

[3] In his analysis of the earliest Irish Republican terrorists, Clutterbuck (2004, p. 169) uses this approach to point out that the assumption those groups didn't attempt to kill many people is incorrect:

> To infer from the low level of actual casualties that Clan na Gael therefore actually attempted to minimize them is to confuse their failure to kill anyone with a desire not to do so. It also shows a lack of understanding of the lethal effect of dynamite when it is detonated in enclosed tunnels, buildings or places of public resort. Their primary objective may not have been specifically to cause large numbers of dead and injured but only good fortune prevented casualties occurring as an inevitable consequence of their actions.

[4] Considering success and failure from the terrorists' perspective can be easy or hard depending on the group. Definitions of success differ considerably from group to group. For some, simply the fact that an operation was attempted—that they demonstrated their continuing ability to act—might constitute a success, whether or not it achieved any particular outcome. For others, particular destruction levels might be needed, and anything less than a threshold would be viewed as a failure. Different elements within the same group may have different definitions of what constitutes success (see, for example, overview in Jackson, et al., 2008). How difficult—and speculative—it is to determine a group's success criteria depends on the group: Some groups make their standards relatively clear and public, others do not. Some focus on tactical details, e.g., the Provisional Irish Republican Army's (PIRA's) success criteria were focused on security-force causalities, economic harm, the minimization (at least formally) of civilian casualties, the public reaction to an operation, and the operatives escaping unscathed (see, Jackson, 2005a, pp. 112–113). Others have focused on trying to maximize relatively abstract things, including the display of tactical skill by the group. For example, Johann Most was quoted as suggesting, "The more highly placed [is] the one shot or blown up, and the more perfectly executed the attempt, the greater the propagandistic effect" (Miller, 1995, p. 44).

A further complication is that, like other organizations, terrorists sometimes attempt to revise what they "meant to do" after seeing what actually occurred—either to make their actions seem more successful or to counter criticism that they went too far. For example, in his discussion of mass casualty bombings, Quillen notes,

> Of course, it is not always clear the terrorists intended to kill such large numbers of people. As a practical matter, terrorists who place a bomb on an airplane can reasonably be suspected of seeking the death of all of its passengers. In other attacks, however, it is not nearly so easy to determine the group's intentions. Just as terrorists sometimes kill fewer than intended, no doubt on occasion they kill more. Terrorists often claim such a "mistake" when their supporters and potential supporters express displeasure at an especially high body count or they fear a harsh government reprisal (2002, p. 281).

the attack was designed and executed. This dual focus captures elements of both what terrorists are trying to do (produce tactical results that they believe will advance their interests and help them achieve their goals) and what security organizations are trying to do (limit groups' abilities to produce those outputs). In doing so, it sidesteps the question of from whose point of view success and failure should be assessed, and it simplifies the analysis by staying clear of factors that may shape the broader strategic impacts of individual terrorist attacks.

A tactical focus also makes it possible to avoid considering success and failure in a binary way because at the tactical level, operations can be "partially successful" (i.e., although they may produce outputs that are less than what they might have been, they did not break down completely). The tactical level is also the point at which more—though certainly not all—of the relevant variables are within the control of the attackers. As a result, the characteristics of those attackers, their planning ability, their capabilities, and their ability to overcome security measures are primary drivers. The tactical level is also a predominant target of security planners, and so understanding how operations go well or poorly at that level is clearly relevant to informing future planning.[5]

The remaining sections of this paper: (1) describe our three-component framework, which uses the concept of matches and mismatches between different components to explore the key relationships and interactions that drive success and failure of operations; (2) provide a more detailed discussion of the components of the framework; and (3) discuss its relevance for thinking about security planning and counterterrorism analysis.

The Terrorists, What They Are Trying to Do, and the Security Forces Opposing Them: Using the Idea of "Matches and Mismatches" to Frame Drivers of Success or Failure

In examining the success and failure of terrorist operations, previous studies have looked at correlations between data on the results of terrorist attacks and various group characteristics (e.g., size, resources, state sponsorship, size of the attack team, weapons and tactics, and so on as referenced earlier).[6] Other research efforts have examined case studies of terrorist operations

[5] Throughout this paper, we use the terms *terrorist* and *terrorist group* to describe nonstate violent groups whose operations' success and failure is of interest to security planners. An additional consequence of our focus at the tactical level and on the factors that make particular attack operations more or less likely to succeed is that the framework we describe can be applied more generally to the violent activities of other groups, including to components of insurgencies where the security organizations opposing the non-state actors may be traditional military forces. As a result, we draw on examples from groups that have used terrorist or insurgent tactics at different points in their operations. However, for ease of presentation, we use the terms terrorist and terrorist group throughout the discussion.

[6] Many of these types of correlational analyses have been hindered by the serious data limitations that exist with respect to terrorist-group behavior. While there are a variety of databases in which information on terrorist attacks has been collected, their utility for assessing why operations succeed and fail is limited. In many cases, failed attacks are underrepresented or absent from such datasets. Their exclusion is in some cases intentional, with failed attacks falling outside the collection efforts' criteria for inclusion. However, because terrorist attacks can fail "invisibly" (i.e., operations may break down in ways where their failure is either not known outside the terrorist group, invisible outside security organizations, or not reported in the media sources that are the central inputs for terrorism databases) undercounting would be inevitable even in data collection efforts that sought to include failed operations. It is also the case that incident datasets often do not contain the type of contextual and descriptive data that is needed for understanding how the characteristics of two operations that otherwise look very similar (e.g., one successful and one failed assassination) may have differed. Paradoxically, the more common terrorist attacks are in a given area—regrettably resulting in larger sample sizes for study—the less detail is reported in the

in detail and constructed lists of variables relevant to thinking about why particular operations went well or poorly. For example, the recent Homeland Security Institute analysis on this subject cited factors including the level of the terrorists' training, technical sophistication, operational proficiency, level of operational security, whether the attackers were known to security organizations, the level of innovation of the operation, whether the attackers encountered technical difficulties, whether access to the target was restricted, how much law enforcement knew of the plot, the restrictiveness of the security environment, the amount of information sharing and international cooperation among security organizations, and the level of vigilance of the public and security services (Homeland Security Institute, 2007, pp. 16, 54).

Though this past work provides a starting point for analysts seeking to anticipate future terrorist behavior, we have found it difficult to apply such lists of factors in analyses focused on prospective security planning. In particular, a framework for relating factors to one another and for guiding the thinking of analysts and planners in considering their relative importance is missing, which can result in factor lists that mix group characteristics and processes that affect those characteristics (e.g., attackers' operational proficiency and whether or not they trained for the attack, where the latter is a process that affects the former), duplication of factors in some or in part (e.g., how well the attackers were able to hide the plot and whether security services were aware of it), and difficulty in considering tradeoffs that attack planners make (e.g., the benefit of staging an innovative or unusual operation versus risks of attempting an attack the group might not be very good at staging).

We also believe that such factor lists do not reflect the fact that the probability of success of terrorist operations is usually not driven by the *absolute value* of particular factors but rather by how those levels *compare* with what the terrorist group needs to bring its plans to fruition. Put more concretely, it does not matter if a terrorist cell possesses the level of operational skills that would allow it to carry out precision sniper operations if the attack it is planning is simply to walk into an airport and open fire with automatic weapons; it does not matter if a terrorist cell's operational security skills are terrible if the security services it faces lack the capability to detect the terrorists under any circumstances; and it does not matter if the defenses around the terrorists' intended target are exceedingly tight if the terrorists can render those protections irrelevant by selecting an appropriate attack mode or simply by their level of skill and professionalism.

To remedy this shortcoming, we constructed a simplified framework that relates the types of factors that have been proposed in the literature to one another—and to how they act in concert to shape the likely success or failure of a terrorist operation. The framework is structured around three sets of characteristics:

- terrorist group capabilities and resources
- requirements of the operation it attempted or is planning to attempt
- relevance and reliability of security countermeasures.

The heart of our argument is that it is not the absolute values of any of the characteristics that fall into these classes that are important for understanding the likelihood a terrorist opera-

media and by other sources about each attack. As a result, even while more data points are theoretically available, they may not be useful for these types of study.

tion will succeed or fail, but the relationships between them.[7] We have thought about these relative comparisons in terms of *matches* and *mismatches* between the different classes of factors (illustrated in Figure 1).[8] In general, the chances of an attack succeeding increase when (1) the characteristics of the attackers closely match the characteristics of what they are attempting and (2) when there is a mismatch between those characteristcs and the security or protective measures the attack must overcome.[9] So,

- If a group is attempting an operation that is well *matched* to its operational skills, knowledge of its intended targets, its technical capabilities, and so on (e.g., a group that has staged 100 bombing operations is planning another similar operation), then its chances of success are higher than if it was attempting something *mismatched* to its skills and capabilities (e.g., that same group is attempting a chemical weapons attack at a target type it has never attacked before).
- When there is a *mismatch* between a terrorist group and the security forces opposing it (e.g., the police force lacks sufficient technical or other ability to penetrate the group's operational security measures), the terrorist's chances of success are much better than if there is a *match* between them (e.g., the police force—through whatever means—can routinely identify the group's members.)
- Success is more likely if there is a *mismatch* between its planned operation and the relevant security forces or protective measures (e.g., the group is using an attack mode that intelligence and security measures have not been designed to detect or defeat) than if there is a *match* between them (e.g., the group is using weapons and tactics that are already addressed in security and defensive plans).

In this discussion, our use of language emphasizing that there can be differing degrees of match and mismatch is deliberate. Good correspondence between a terrorist group's skills and the attack they want to carry out increases the chance of success, but in most cases success will never be assured. We are, therefore, really talking about levels of *operational risk* (i.e., how factors increase the chances that it will succeed or fail, not how factors deterministically

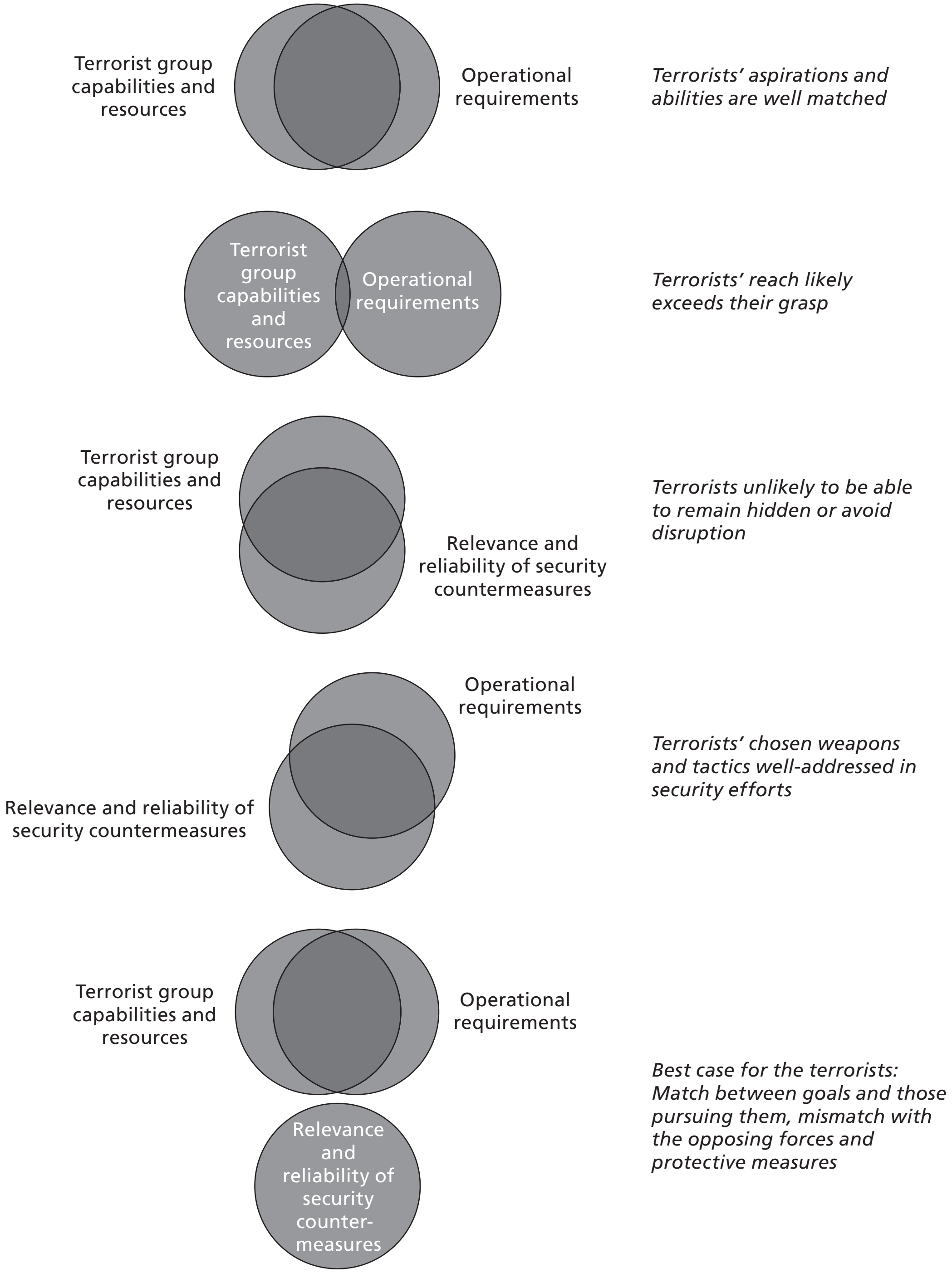
[7] These three general categories could be used to organize more detailed or specific factors about groups, operations, or security forces (e.g., the group's level of tactical or operational security skills, to select two identified in past studies), but the central point of our framework is not to organize the many factors that have been identified previously into simpler overarching categories but rather to focus on relationships between factors rather than those factors in isolation.

[8] Precedents for framing this sort of analysis in terms of matches and mismatches can be found in the terrorism literature. For example, Drake (1998) discusses these issues with respect to technical abilities of terrorist groups:

> The technical ability of terrorists varies considerably. It is not necessary for somebody to be well-trained in military techniques for them to be able to carry out certain types of terrorist operations. *Uncomplicated attacks against relatively undefended targets do not require much in the way of training. . . . However, for terrorists wishing to carry out more complex operations, training in the use and construction of weapons is extremely useful* (pp. 80–81, emphasis added).

[9] This concern with matches and mismatches between security forces/protective measures and potential attackers echoes similar discussions in the literature on policing for criminal activity other than terrorism. For example, for many years, there has been concern regarding the potential mismatch in firepower between criminals (particularly criminal organizations with the resources to acquire automatic and other weapons) and the law enforcement organizations that oppose them. Such concerns can be traced back to early discussion of the replacement of police revolvers with semi-automatic handguns (e.g., Kendig and Zumpetta, 1991); more contemporary discussions about the balance of weapons between police and organizations such as drug cartels (e.g., the contemporary discussion of Mexican cartels outgunning the police in Ellingwood and Wilkinson, 2009); and the budget, training, and other requirements for maintaining the match between police capability and criminal activities in new areas such as electronic crime (e.g., Jewkes, 2003).

Figure 1
Venn Diagrams Illustrating the Match and Mismatch of Key Characteristics


Terrorist group capabilities and resources
Operational requirements
Terrorist group capabilities and resources
Operational requirements
Terrorist group capabilities and resources
Relevance and reliability of security countermeasures
Operational requirements
Relevance and reliability of security countermeasures
Terrorist group capabilities and resources
Operational requirements
Relevance and reliability of security counter-measures

Terrorists' aspirations and abilities are well matched

Terrorists' reach likely exceeds their grasp

Terrorists unlikely to be able to remain hidden or avoid disruption

Terrorists' chosen weapons and tactics well-addressed in security efforts

Best case for the terrorists: Match between goals and those pursuing them, mismatch with the opposing forces and protective measures

RAND *OP257-1*

"make" an operation succeed or fail). Even activities that look like they should be trivial for a high-capability group can "go wrong," and even groups that do not know what they are doing will be lucky at times. This fundamental reality is driven by the fact that, in terrorist operations (as is the case for most activities), planners can identify and hedge against many risks, but there will always be variables that are outside of their control.

In the following sections, we turn in more detail to the three classes of characteristics, discuss how factors identified in previous work—both ours and others—fit into each of them, draw on examples from historical terrorist operations to more tangibly illustrate these concepts of match and mismatch in application, and explore how the three different classes of factors interact with and influence each other. The goal of this exercise is to construct a consistent way of thinking through the different factors.

Terrorist Group Capabilities and Resources

For a group to successfully execute any action, it must have the capabilities and resources that are necessary to carry out its plans. The resources that shape the success or failure of individual terrorist attack operations consist of the tools the group has (e.g., weapons and other technology), information needed to plan and execute the attack, and access to people with different types of necessary skills.

The *tools* the group has at its disposal contribute to whether its operations will go well. Matching the right technology to a problem—whether that technology is the right weapon to achieve the desired effects at a target or the right communications technology to communicate securely among operatives—can only be done if the organization has those tools at its disposal (e.g., if a group wants to destroy a building, its chances of doing so if it only has firearms at its disposal are lower than if it also has explosives and incendiary weapons). Groups with access to more technologies will have more choices available to them.[10] As will be discussed in greater detail in subsequent sections, it is the match between the technology and what the group is trying to do that is critical. Groups can stage devastating attacks using cheap and simple means, providing that those weapons or supporting technologies are appropriate to the attacks they are attempting to carry out.[11] The reliability of the group's technologies is also important. Weapons that do not function properly during an attack are a recipe for failure. For example, improvised or home-built weapons may or may not perform as predictably as commercially manufactured ones, and so operations using them may be at greater risk of failure.[12] PIRA provides a ready example of this dynamic, as early on in its operational career, its homemade bombs and mortars failed frequently (and often catastrophically), but over time, the quality and reliability of its manufactured devices improved to the point where their reliability rivaled commercial versions (Jackson, 2005b).

The information available to a group executing an attack operation—its *situational awareness*—can also shape the attack's outcome. Situational awareness information is relevant to

[10] For example, focusing on weapons technologies, the Greek terrorist group November 17 acquired and used only a small set of technologies, while other groups, such as PIRA or Hezbollah, eventually built capabilities in a wide variety (see, for example, Jackson and Frelinger, 2008; Jackson, 2005b; Cragin, 2005; Dolnik, 2007; Don et al., 2007).

[11] For example, many suicide operations carried out by individuals on lightly defended targets are far from "technology intensive," requiring only basic explosives and a means for the attacker to detonate them where desired.

[12] Whether the group is aware of the strengths and weaknesses of its weapons and technologies (e.g., whether the group has tested their reliability) also shapes how it plans operations and either does or does not hedge against those reliability risks.

both planning (e.g., how much the group knows about the target will contribute to it making appropriate choices from among its technology options and operatives) and during the operation itself (where new information can provide the trigger to allow the group to adjust to changes in circumstances that might otherwise derail its initial plan). The most obvious examples of the effect of this factor is when groups have the wrong information (e.g., when PIRA staged an assassination at the *former* address of a government official (Drake, 1998, p. 59), though less total shortcomings in group knowledge could reduce chances of success.

For specific operations, both the *number and the quality of the people available* to the group are important. The overall quantity of individuals available to a group determines the pool from which they can draw when deciding how many members are devoted to a particular attack.[13] Large groups (e.g., PIRA, Hezbollah, or the Liberation Tigers of Tamil Eelam [LTTE]) have flexibility in making choices about how many people are devoted to particular attacks. Small groups (e.g., many of the left-wing groups that operated in Europe in the 1970s and 1980s, individual cells of al Qaeda, or other loosely networked groups) can be forced by the size of the pool of members available to have all their members participate in a planned attack, and their total membership represents a hard upper constraint on their operational capability. Echoing the discussion of matches and mismatches above, the effect of human resource characteristics on operational success depends on matching the quality and quantity of people to what the group is attempting (discussed in more detail below.)[14]

The quality of the human resources available to a group (or on the attack team carrying out a specific operation) is determined by the skills of the individuals in a range of areas. In some ways, the influence of attackers' *technical skills* on the success and failure of operations is easiest to understand. Just knowing how to fire a gun is different than being able to use it accurately, which is different from being able to carry out sniper operations, which yet again is different from being able to successfully provide supporting fire in multi-attacker teams.[15] Weapons of differing levels of complexity require different levels of technical skill to use them effectively.[16] Shortfalls in technical skills can produce, depending on the weapon involved, reductions in accuracy (probability of a hit), the type of effect on a target (e.g., strike to stop a vehicle vs. destroy it), and the probability of achieving the desired effect given a hit.[17] Other technical skills can be important as well. For example, for an attack that relies on the terrorists

[13] For example, see Drake, 1998:

> The size of the terrorist group will also determine, to a degree, the complexity of the operations which they can carry out. Relatively simple operations such as assassinations, mass-casualty bombings, and similar attacks do not require the participation of many terrorists. However, an operation such as the abduction of a high profile person is more complex and requires an assault team, somebody to sort out the logistics such as transport, safe houses, and possibly any subsequent communications with the authorities or any other interested parties (p. 80).

[14] For example, how "high quality" (in skills, knowledge, and so on) an individual terrorist is will depend much less if the role that individual is intended to play is to act as a suicide bomber than if the group wants him to be the triggerman in a sniping operation. As a result, successful suicide attacks have been staged with individuals of comparatively limited capability. That said, previous analyses have suggested that *degree of success* in suicide operations still appears to correlate with certain measures of human resource quality such as education (Benmelech and Berrebi, n.d.).

[15] For example, looking at assassination operations, Fein and Vossekuil (1999) examined different levels of weapons experience that attempted assassins had at the time of the attack.

[16] For example, Sharif (1996) identified differences in success (as defined) and the type of weapon used for the attack.

[17] Questions about differences in operational skills go back to some of the earliest theorists of terrorism, for example Miller paraphrases Johann Most as advocating that "All weapons are useful, but only if one knows how to use them. Too many

flying an airplane or digging a tunnel to access the target,[18] whether or not the attackers have the skills required to do so becomes important.[19]

But success in carrying out an attack requires more than just the technical ability to use a weapon well. Groups also require *operational security skills* to operate clandestinely and to hide their operatives from the attention of security organizations that may be looking for them.[20] Some groups are much better at doing such things than others (Bell, 2000).[21] The individuals' skill in *planning* operations[22] (e.g., the skills required to make the right choices about how many operatives to devote to the attack, how much financial or other resources are allocated to it, what weapons will be made available, or how much preparation time is needed) also shapes the chance of success.[23] The ability of the group to manage the operation once it is initiated—

revolutionaries 'have paid with their lives' for having attempted to use a weapon 'without first having made himself a marksman'" (Miller, 1995, p. 45).

[18] A dramatic historical example of these technical challenges comes from the Euskadi Ta Askatasuna [Basque Homeland and Freedom movement, or ETA] assassination operation on Admiral Luis Carrero Blanco, as described by Bell (2006, pp. 253–254):

> The way the four had chosen was to tunnel out under the street and then dig a chamber that would be filled with explosives. When Carrero's car passed over the mine, guided in place by a double parked car, the explosives would be detonated electronically from a distance. It was a complex project, perhaps unnecessarily so; and in their year of preparation and surveillance, the four had shown themselves less than highly advanced skilled professional revolutionaries. . . . The pickaxes from the Basque country were too large. One digger suffered from claustrophobia. The first shovelfuls of dirt taken from beyond the wall were permeated with escaped gas and sewage overflow. . . . There was a landslide. They found a technical manual in a bookstore but propping and piling seemed to be associated with larger tunnels. They kept going, carrying their pistols so that if trapped, they had an alternative to asphyxiation by the gas fumes.

In addition to demonstrating the skill requirements for more sophisticated attacks and the problems that can arise when they are lacking, since the attack was successful, this case also demonstrates that even unskilled attackers can be lucky.

[19] In an analysis of commando operations, Hoffman (1985) determined that personnel skill level was a significant determiner of operational success: Elite forces were more likely to succeed than irregular forces.

[20] While many groups can acquire a level of operational skill to maintain a level of secrecy over their actions—e.g., basic communications security and other tradecraft described on al Qaeda/jihadist Web sites and in manuals (see Ilardi, 2009)—some groups get good enough that they can hide the activities of operatives that authorities already know are terrorists. For example, PIRA reportedly staged the death of some of its members and stole some police files to try to reconstitute their operational security (Coogan, 1993; Canadian Security Intelligence Service, 1994; McGartland, 1997).

[21] See discussion in Burton, 2006 of the operational-security skills implications of al Qaeda becoming a more dispersed group. Marking the continuity of this factor as an importance, operational security skills (coupled with the lack of skills of the police forces facing them) has also been cited as a factor in the sustained operational successes of the earliest Irish revolutionary terrorists (Clutterbuck, 2004, p. 168).

[22] Operational planning skills can vary considerably among different individuals—e.g., see, Drake's (1998, pp. 74–75) discussion of the "quality" of group leadership. In fact, most individuals are far from perfect in making such choices. Drake's (p. 163) further discussion of terrorists' choice of targets and the processes involved in doing so summarizes this succinctly: "When examining the actions of terrorists, one must bear in mind that one is dealing with people, with all their imperfections and unpredictability, rather than some hypothetical, hyper-rational beings."

[23] Reflecting our language of matches and mismatches between factors, this factor might also be termed the group's "matching ability" for aligning its capabilities with the operations it wants to carry out. In our previous work, we have drawn a distinction between two different types of such matching ability: (1) a group, given a set of resources and skills on hand, picking an operation that matches them and (2) a group, having selected an operation, assembling the resources and skills needed to carry it out (Jackson, 2005b, pp. 113–117). Hoffman (1997) illustrates the importance of this capability for groups using the words of George Habash, "The main point is to select targets where success is 100% assured."

the *command and control or leadership skills* of the operatives involved[24]—is then a driver of whether its plan can be put into operation. Different types of operations require different levels of these skills; e.g., managing multiple attack teams in a simultaneous attack is harder than a simple, one-team operation. In all of these areas, whether a group is "good enough" to do what it wants is of primary importance, but its skills and capabilities also drive whether it will be able to improvise and adapt during operations when circumstances change or when they encounter obstacles (see, for example, Jackson et al., 2007).

Our discussion of group capabilities has taken an explicitly static view: In assessing success and failure, the focus must be on the attack team's characteristics at the time it is staging the attack. Our focus has also been on the individuals involved in the attack—their technical skills, planning skills, and so on—rather than thinking about the terrorist group overall. *Organizational* characteristics (e.g., the group's ability to maintain these skills) as opposed to *individual* ones will largely determine whether a terrorist group can sustain success over time from operation to operation (see, for example, discussions in Jackson, 2005a, and Jackson et al., 2005). However, when the focus for a given attack is on the tactical level, the characteristics of the specific individuals who are involved dominate.

We have excluded a number of *processes* that have been included in some past efforts to examine terrorist success and failure. For example, it might be argued that a groups' ability to acquire new weapons or whether or not it engages in training before an attack will affect its outcome. While those activities are important, when considering the potential outcome of individual operations, we view them as ways groups can affect the values of the characteristics discussed above rather than as factors in their own right.

The importance of separating out these processes is easy to demonstrate. For example, it is clear that the skill of the members of an attack team is important for success. To try to increase those skills, they could train before the operation (e.g., shooting practice at a firing range). If the training is both appropriate and effective, the group's skill will go up and the chance of success will indeed be increased—but the relevant variable is the increase in skills, *not* the training. But, if the training is inappropriate or poor (e.g., it is based on wrong information or carried out by individuals who don't know what they are doing), it will make no positive contribution to the chance of operational success.[25] As a result, interpreting the fact that training occurred as necessarily increasing an operation's chance of success may lead one to draw exactly the wrong conclusion. It is not the presence of the *process*, but the presence of its *successful outcome* that is a determining factor.

[24] *Command and control* as conceptualized here includes the influence of leadership over other group members, not just hierarchical command and control (Jackson, 2006). This broad definition of command and control in terrorist groups has been recognized for some time. For example, see discussion in della Porta, 1995 and Strinkowski, 1985, pp. 94–99, that explains the limits of hierarchical control in such groups. Drake's discussion of "leadership quality" is also relevant (1998, pp. 74–75).

[25] For example, in some terrorist groups, a core purpose of training is ideological indoctrination rather than skill acquisition. In those cases, the contribution of training to the success of a specific operation would be questionable. Other examples include the training of some groups by state militaries, in which the information transferred to them was inappropriate to their operational situation and therefore potentially detrimental rather than beneficial (see discussion of numerous groups' training regimens in Forrest, 2005).

Other relevant processes include[26]

- *intelligence gathering and surveillance* to increase situational awareness or help improve operational security practices
- *recruiting for people with needed skills or knowledge* to increase total human resources or improve their quality
- *technology acquisition, production, development, and testing* to increase available technology or improve its quality
- *operational training and mission rehearsal* to improve planning and other operational skills[27]
- *weapons training or testing* to increase technical skills and assess technology quality and reliability.

Groups differ in their ability to carry out all of these processes (see, for example, case studies in Jackson et al., 2005).

Operational Requirements: What Do They Want to Do?

Though thinking about terrorists' chances of success and failure usually focuses on the nature of the group or individuals involved, whether they are "good enough" to stage a particular operation depends on what they are trying to accomplish. Some terrorist operations are much harder than others. Walking to an unguarded target and painting a slogan on a wall (such as operations typical of the Earth Liberation Front on commercial targets) is far easier than fabricating and then placing explosive devices undetected on a public passenger train and escaping before they go off (e.g., the Madrid train bombings in March 2004). A group whose aims and aspirations are limited to the first activity would have a much lower bar for success than a group attempting the second. Put in terms of our language of matches and mismatches, more groups' capabilities would match the first than the second type of operation.

To understand terrorist success and failure, we therefore must understand the characteristics of different operations that make them difficult or risky—and also therefore must raise the bar for group skills, technology, and so on. The requirements of an operation are driven in large part by the *tactical outcome the group wants* and the *type of target* they are attacking. Groups have attempted to destroy targets, to cause mass casualties in various ways, to take and control sites, to seize and hold individuals, and so on.[28] Some operations have sought to kill as many people as possible with little discrimination, while others have sought to kill some but not others, or avoid killing anyone at all.[29] The nature of what groups are seeking to accomplish

[26] See the summary in Hoffman, 1997, and the discussion of group organizational learning, innovation, and adaptation in Jackson 2005b; Jackson et al., 2005; and Jones, 2006.

[27] See, for example, the description of the preparatory activities of the July 7, 2005, attackers in Kirby, 2007, p. 425.

[28] This diversity of potential objectives means that a would-be attacker might have a wide variety of acceptable outcomes for an attack and might not always optimize for a particular effect.

[29] Examples of operations that ended up killing individuals the terrorists did not intend to, with concomitant damage to public opinion regarding their causes and interests, are readily available from groups across the ideological spectrum, ranging from the PIRA's bombing of a Shankill fish shop that killed a number of civilians (Silke, 2003) to a case where Egyptian Islamic Jihad, led by Ayman al-Zawahiri, killed a young girl in a failed assassination attempt on Egyptian Prime Minister Atif Sidqi, which Sidqi describes in his influential book *Knights Under the Banner of the Prophet* (Brachman and McCants, 2006). See also the discussion of planning of various assassins and their sensitivity to collateral damage in their attacks

determines their requirements for information, technology, people, and what expertise they need to have to achieve those goals.[30] Destroying a building has vastly different requirements than storming and holding it for an extended negotiation. If a group wants to kidnap a public figure, the operation will have different requirements than attempting to assassinate him or her. Seizing a nuclear power plant to shut it down is different from seizing a movie theater to shut it down. The effects the group wants to achieve must match the capabilities of the weapons and other technology they have available, and the nature of the operation needs to match the skills and information possessed by the attack team, which must also be large enough to carry out the attack.[31]

The *complexity of the operation* also shapes what is required to execute it successfully.[32] Simple operations (e.g., an attacker walks to an undefended target, plants a bomb and leaves) require less skill than more-complicated attacks relying on multiple attack teams doing different things in sequence or simultaneously.[33] The more complicated the attack plan (i.e., the more "moving parts" it has, where each part must be successful for the attack overall to succeed),[34] the greater operational finesse a group needs to execute it successfully.[35] For example, in a past analysis of historical commando operations, Hoffman (1985, pp. 13, 18–20) cited complexity

in Bell, 2006 (p. 235). With respect to groups attempting to stage bombings but avoid casualties by providing warnings, Coogan (1993, p. 289) observes: "It's one thing to phone a warning, it's another to estimate how soon it will take effect."

[30] See Meyer et al., 1993, for a discussion of both goals and match of weapons to targets. Jenkins et al. (1977, p. 12) makes estimates of the personnel requirements for kidnapping operations versus barricade and hostage situations—where the average for a barricade and hostage (usual minimum of approximately three, average between five and six) is less than for a kidnapping (average between six and ten people).

[31] A related question that shapes the likelihood of success of an operation is how sensitive the desired outcome is to deviations from perfect execution, technical breakdown, or other types of shortfalls. Is the result complete failure (e.g., a shot is taken and missed, a bomb doesn't go off)? Partial failure (e.g., the bomb goes off but it produces less damage)? Or is there little or no effect on the outcome? At the risk of restating the obvious, operations where the tactical outcome is insensitive to mistakes or other shortcomings of the attacking force will be more likely to succeed than those whose requirements are more stringent.

[32] In the literature, various comparative rankings of operational complexity have been proposed at various times, for example, the distinction drawn by Drake (1998) between operations such as assassinations and mass-casualty bombings from an operation such as the "abduction of a high profile person [as being] more complex" (p. 80). Others present more extensive scales, such as the one proposed by Oots (1986, p. 51), "Simple acts: bombings, sniping, theft or break in, sabotage, and shoot-outs with police; Moderately difficult: armed attacks (with missiles and other weapons), hijacking, and takeovers of non-aerial transports; Difficult: kidnapping, barricade and hostage, and facility occupation." No additional information is provided on the basis for grouping the operations this way.

[33] Suggesting the relationship between the nature of an operation and resource requirements, Oots (1986, pp. 69–72) identified a correlation between the difficulty of the terrorist attack and the size of the acting group involved in carrying it out.

[34] Sometimes even two moving parts are too much:

> A more recent example occurred in an Irish attempt on Field-Marshal Sir John French. The plotters planned to place a rented cart in the road to stop French's convoy and make it vulnerable to a sneak attack. Unexpectedly the cart proved clumsy, and as they struggled to get it into position, a constable appeared telling them to let the convoy pass first. One conspirator panicked, throwing a grenade at the constable, thus saving the Field-Marshal's life (Rapoport, 1971, p. 20).

[35] Michael Levi makes a related point with respect to a terrorist carrying out all the steps required to stage a nuclear attack: "It has often been said that the defense against terrorism must succeed every time, but that the terrorists must succeed only once. This is true plot to plot, but *within each plot, the logic is reversed. Terrorists must succeed at every stage*, but the defense needs to succeed only once" (2007, p. 7, emphasis added). While Levi is making the point with respect to the actions of security forces (discussed later), the same logic applies to the terrorists' actions as well.

of the attack as a factor related to the success of the operation.[36] The more "tightly coupled" the parts of an operation are (i.e., the shorter the time period they must occur in or how quickly they must occur in sequence[37]), the more difficult the operation will likely be to pull off. When elements are more loosely coupled and there is flexibility in timing or the ability to adjust if one piece of the attack does not go as planned, risk of failure is likely lower (Jackson and Frelinger, 2009).[38] Redundant elements in operational design—where the failure of one or more might reduce the effect of the attack but not cause it to fail—is a way some attackers have hedged against these risks. For example, in an attack employing multiple bombs at many sites (e.g., the 2004 attacks on the Madrid railway system), the failure of some devices to detonate would reduce the scale of the operation but not cause it to fail outright.[39] In addition to raising the skill requirements for attack success, complex operations can also require additional technology (e.g., communications[40]) or the involvment of a larger number of attackers.

Just as some operations are more complex than others, different attacks have different *operational signatures*—some attacks are just easier to conceal than others.[41] One of the advantages cited for person-carried suicide bombs is that, assuming successful concealment of the device under the attacker's clothing, the first clearly hostile action that takes place is when the attack itself occurs. In contrast, planting a bomb requires taking overtly hostile action before the actual attack is triggered.[42] During the period between the first hostile act and the operation itself, there is the risk of detection and disruption. The operational signature defines part of the requirement for the group's operational security skills, where groups seeking to hide

[36] For example, Sharif (1996) identified correlation between terrorist success (as defined) and simpler operational types (where explosives attacks—simplest type—were compared with armed attacks and hostage situations—the most complex).

[37] See, for example, Roggio (2008) for a description of just such an operation where the tight coupling resulted in breakdown of the attack.

[38] The Mumbai armed assault in November 2008 is an example of a loosely coupled operation, where four attack teams operated independently and, therefore, the failure of one team would reduce the scale of the attack but not cause it to fail completely (Rabasa et al., 2009).

[39] For example, it has been suggested that the Madrid bombers intended more of their devices to detonate when they were in the same station to maximize the effects, but one of the trains was late, so the operation did not go completely as planned. Furthermore, of the 13 bombs planted, three did not detonate. Nonetheless, the attack was a devastating one, producing very high casualties (BBCNews, 2004a; 2004b).

[40] However, these additional demands also can potentially create other challenges; e.g., the vulnerability of communications to monitoring can mean that operations requiring more coordination are more vulnerable to security force intervention (discussed in more detail below, see also Enders and Su, 2007; Shapiro, 2007).

[41] In his discussion of terrorist decisionmaking, McCormick (2003) describes groups making trades between the need to remain invisible (i.e., focusing on operational security) against the need to act and have influence (which generally requires a level of overt action). This illustrates how operational signature plays in attackers' calculus as a result of its influence on the chance an operation will be discovered and disrupted.

[42] For example, Clutterbuck's (2004, p. 170) description of different bombing operations used by early terrorists in the United Kingdom and Russia demonstrates such differences: In contrast to the Irish groups, who used time-delay bombs, the Russians'

> primary design concept was to use an electrical charge sent along a command wire in order to detonate the explosive that always consisted of home-made dynamite. This technique required them to have visual contact with the target or through a specifically deployed individual tasked to indicate precisely the moment for detonation. It was a high risk tactic for a terrorist group to adopt as it required elaborate preparations over a long period of time and often involved tunnelling. Consequently, the opportunities for discovery by the police or the public and hence the possible capture of the terrorist were much greater than in the case of the Irish 'place it and leave it' approach.

higher-signature operations need to be more skilled than groups trying to hide less obvious attacks.[43]

For attacks to have a good chance of success, there needs to be a good match between the operational requirements and the capabilities of the group (or portion of the group) seeking to carry it out.[44] The capabilities of very sophisticated groups (e.g, PIRA or the LTTE at their peaks) would have a high degree of match with a wide range of operations, from simple to complex. Smaller, less-organized, less-sophisticated groups (e.g., a "self-starter" cell of al Qaeda sympathizers or an affiliate of the Animal Liberation Front) would be well matched to many fewer operations. In both cases, the group could attempt a difficult, complex attack, but the latter type of organization would have a much slimmer chance of pulling it off successfully than the former one.

This is not a paper on terrorist group decisionmaking, and the reader is cautioned from interpreting our discussion of matches between capabilities and operational requirements as suggesting that terrorist organizations plan operations this way. What we are describing is a framework for assessing operations and anticipating their likelihood of success and failure, not a model of terrorist attack planning.[45] That said, a brief observation on how matches and mismatches could be recognized in a group planning process are relevant to help frame some relevant observations for counterterrorism. As groups plan attacks, more-methodical groups will make resource application decisions in an effort to execute a desired plan. Those decisions may be constrained by the number of people the group has, their knowledge, or other resources. In that decision process, consideration of what the group *wants* to do may make important mismatches apparent to the attackers that cause them to either alter their plans or to seek to correct the mismatch through the various processes discussed above. The operation to carry out the terrorist attacks of September 11, 2001, provides a ready example of this effect. The attackers clearly made a decision that running their operation without trained pilots would risk the success of the attack, so they pursued training (adding an additional process to the preparatory stages of their operation) to correct that mismatch. Certainly not all terrorist groups are systematic or deliberative enough that they would notice such potential mismatches, nor would all groups choose to do anything about them if they were noticed. Some groups are more tolerant of mismatches (i.e., residual operational risk) than others.[46]

[43] Rapoport (1971, p. 19) generalizes that a longer length of time between any preparation and execution of the attack increases the probability of failure.

[44] The nature of the planned operation largely determines the requirements that they have to meet in human resources, knowledge, technology, expertise, and so on to be successful. However, there are a variety of resource mixes or "force packages" that might result in comparable chances of succeeding at a given attack. Numbers of people, their skill levels, technology, and information can be traded off against one another—e.g., an attack might be successful with only a small number of highly trained individuals (the terrorist equivalent of a Special Forces team) but might require a much larger contingent of untrained foot soldiers. Other substitutions are similarly possible, e.g., substituting attack technologies that have large areas of effect for more precise weapons to obviate the need for exact targeting information, etc.

[45] Though there are some terrorists and terrorist groups that do plan that way, most do not. Some groups stage operations with relatively little planning and lack the self-awareness regarding their own capabilities to make reasonable assessments how their strengths or limitations shape the chance of their operations of being successful. Others are more sophisticated, though they may still be limited by key resources, assumptions, preferences, or prejudices that constrain the ways they make choices. Either type of group might attempt an operation that was poorly matched to its capabilities and, for the purposes of applying this framework for understanding that that operation is not likely to go well, the exact reason why it chose to move forward is less important than the fact that it did so.

[46] For example, see discussion in Phillips, 2005; Hoffman 1997.

As the 9/11 case demonstrates, those preoperational processes may generate signatures of their own, which may or may not be recognized as hostile by security organizations (e.g., the controversy whether the hijackers' training should have been detected as a threat because of their focus on flight but not landing). Another example of this dynamic include groups seeking out individuals with appropriate technical training to produce particular types of weapons, but that seeking activity potentially increases the chance of the plot's detection, even if it might address the technical mismatch the group identified (discussed in Levi [2007, p. 8] with respect to nuclear weapons).[47]

Relevance and Reliability of Security Countermeasures

The law enforcement and intelligence organizations that are opposing a terrorist group—and the specific protective measures in place at the targets they are attempting to attack—can clearly have a significant effect on operational success and failure. These elements can either (1) halt an attack completely or (2) limit its effects by making it go off target, reducing the damage it causes, or rapidly containing and addressing its consequences. While the potential effect of such measures has been recognized in past efforts to understand why terrorist operations succeed or fail, dealing with them in more than a qualitative way has been difficult. For example, the lack of public information on counterterrorism efforts in specific cases means that such measures have sometimes been treated very broadly, with analyses using overall measures such as the intensity of intelligence activity in a country or the presence of particular counterterrorism efforts as a proxy for their likely effect on individual operations. Our framework of matches and mismatches provides a means of proceeding a step beyond such general characterizations to explore the relevance of particular counterterrorism efforts to particular threats—i.e., the greater the match (the overlap in Figure 1) between the intelligence or security activity and the terrorist group or its operation, the greater the chance it will contribute to its detection or disruption.

But answering the question of how security measures or counterterrorism activities match a threat requires an understanding of what drives their effects on a terrorist plot in progress. Some protective measures require the knowledge that the terrorists are there before they can respond to the threat—e.g., you cannot secure a warrant for a person's arrest without knowing who they are and what to arrest them for. Those measures' ability to provide security against future plots depend on two things: our chance of detecting plots successfully and our ability to act on that information once we have it. Other measures are "on all the time"—e.g., an air filtration system in a public building will help reduce the effect of a biological release whether or not we know that release happened. In those cases, their effect on success and failure does not depend on detecting an attack first.

Is the Terrorist Activity Detected? Many defensive approaches for terrorist threats depend on being able to detect the preparation for or initiation of an attack. Stopping attacks before they occur is fundamentally limited by detection capabilities, since if the attackers successfully hide their activities, security forces do not know they need to engage them. Once a bomb goes

[47] These additional processes that groups might choose to go through in preparation for an operation are clearly relevant and important for law enforcement or intelligence detection of the group and its intentions, and could create opportunities for preempting initiation of the operation itself. But we view that as best treated as analytically separate from the consideration of factors that shape likelihood of success and failure of the operation itself, to prevent double counting and convolution of processes and organizational characteristics.

off, it is relatively clear an incident is in progress. There are some exceptions—e.g., clandestine release of a biological agent—where the ability to detect that an attack is in progress is still a concern. Different attacks vary in how easy they are to detect. But even if the characteristics of an operation make it highly *detectable*, that does not imply certainty that it *will be detected*.[48] Security or protective efforts that rely on detection must have the capabilities to collect the information they need and the ability to use that data to recognize the presence of a threat.[49] If detection efforts are "looking for" a threat and have the capability to detect it, that match indicates they could reduce the attackers' chance of succeeding.[50] If they are not, they may not affect its chances at all.[51]

What determines match and mismatch in this case is similar to the factors that shape the terrorists' chance of success, but here the focus is on the characteristics of the security forces opposing them: whether the organizations protecting relevant targets have enough appropriately skilled people,[52] technologies,[53] and even other useful situational-awareness information (e.g., that individuals known to have participated in past attacks have entered their area of responsibility) that will enable them to both collect the additional information necessary and interpret it correctly to recognize the presence of the threat.[54] Skilled and capable security organizations that are well matched with current threats will cut those attackers' chances of

[48] For example, even canine detection of explosives—one of the central modes of detecting bombs and an approach optimized for doing so—is not successful 100 percent of the time (see, for example, the results of an evaluation of a canine explosive detection program in Department of Energy, Office of the Inspector General, 2007). Analogous points could be made about the effectiveness problems in weapons detection screening in the air transportation system where covert testing has demonstrated simulated weapons can frequently pass through checkpoints undetected (Kutz and Cooney, 2007; Frank, 2007; Goldberg, 2008).

[49] These capabilities are similarly related to the chance that the other processes groups might choose to go through in preparation for an attack—intelligence gathering, training, weapons development, and so on—are detected. As Rapoport (1971, p. 18) observed, "Most conspiracies fail in the preparation phase when plans are still being formulated. The possibilities of being detected are multiplied by the numbers involved and the time necessary to perfect the plans."

[50] Use of terrorist watch lists is a simple example of an intelligence and security measure the effectiveness of which is reliant on there being a match between what the defense is "looking for" and the threat. If a terrorist's name is on the list, he or she could be detected; if it is not, he or she will not be detected. See Government Accountability Office, 2006, for a discussion. Certain profiling techniques are another example; in the case of profiles, if the terrorist can identify what is being profiled, an operative who does not match can be selected and a mismatch between the defense and the threat created (Jackson et al., 2007).

[51] See National Academies (2004) for a discussion of explosives detection, the chemical characteristics of explosives, and the ways that particular explosives either do or do not match what specific explosive detection technologies are "looking for." Jenkins and Butterworth (2007) include a similar discussion focused on the strengths and weaknesses of different screening approaches for individuals as a detection mechanism.

[52] A simple example of this need for match is discussion of the shortage of foreign-language speakers in many relevant security agencies in the years since the 9/11 attacks. See Aid (2003) for a discussion.

[53] For example, the controversy whether or not data mining is an effective detection technology for intelligence agencies attempting to identify terrorist plots—in our language, whether its capabilities are well matched to the challenge of detecting known or unknown terrorist operatives and their activities (National Academies, 2008; DeRosa, 2004; Technology and Privacy Advisory Committee, 2004; Jonas and Harper, 2006).

[54] See, for example, the early stages of our model for understanding the effectiveness of domestic intelligence activities (Jackson, 2009).

success; poorly resourced or incompetent security organizations—or ones that are "looking in the wrong direction"[55]—will not.[56]

In evaluating why a past attack succeeded or failed, the analyst can ask a number of questions: What was known about it? When it was known? and Was it recognized as hostile by the organizations involved? Such analyses are standard features of "post assessments" after attacks occur and can be used to specifically examine how well measures that were in place matched the threat. For example, as mentioned above, the flight-school preparations of the 9/11 hijackers were recognized during assessment after that attack, thus identifying a situation where information was available but not correctly identified as hostile activity (National Commission on Terrorist Attacks on the United States, 2004, pp. 83, 272).

The possible effect of security organizations' detection capabilities on the likelihood of success and failure of *future* terrorist attacks must necessarily be more speculative. While it is easy to project how extreme combinations of intelligence or detection capabilities might affect the success of future terrorist operations, for more realistic mixes of capabilities, the question has to be approached categorically (i.e., the analyst must ask how the amount and mix of intelligence, analysis, information collection, and other detection resources do or do not match the range of possible future threats).[57] As a result, in examining these issues, past studies have frequently focused on what we have previously labeled *processes* to rate the potential contribution of security forces to disrupting a terrorist operation. For example, the Homeland Security Institute (2007) study on reasons for the success or failure of terrorist attacks included as factors whether security organizations have broad authorities to gather information, whether information is shared among security organizations, the level of vigilance of the public and security organizations related to terrorist threats, and whether the organizations receive information from other countries' intelligence or law enforcement organizations.

Though prospective analyses are largely limited to thinking in relatively general terms about counterterrorism and security measures, the caveat implicit in the previous discussion of the terrorists applies here as well. While the *presence* of the process may be a necessary condition for success, it is not a *sufficient* one. For example, just because the public is reporting information to security organizations about perceived terrorist activity, whether that reporting affects the chances of success or failure of any real terrorist operations depends how good the data is, whether irrelevant data so dominates that the good data will never be discovered even if it is reported, and that security or law enforcement organizations have the wherewithal to assess the information stream and make use of it.

Are Measures to Act Against the Terrorist Activity Effective? For security and protective measures to affect the likelihood of success or failure of a terrorist operation, the fundamental

[55] For example, one of the explanations why Aum Shinrikyo was able to operate for as long as it did pursuing chemical and biological weapons was a view by relevant security organizations that a religious group like Aum was not a threat (Parachini, 2005). See also the discussion of intelligence activities before September 11, 2001, in *The 9/11 Commission Report* (National Commission on Terrorist Attacks on the United States, 2004).

[56] For example, it has been argued that one of the reasons the LTTE could operate at the high level they did for so many years was the limited skills and poor capabilities of the Sri Lankan military forces opposing them (Jackson et al., 2007, p. 62).

[57] For example, a case where detection and intelligence efforts were extremely well matched to the group was late in the conflict between the British Government and PIRA in Northern Ireland, when the extensive information on PIRA available to security forces gave them the ability to disrupt or otherwise halt a high percentage of the group's operations (Jackson, 2007).

question is, what can they *do*? Whether or not measures are in place, if they are not *effective*, they will have little impact on whether terrorist operations will succeed or fail.

The efficacy of protective measures that *do not* require the detection of a specific attack to affect terrorists' chance of success depends only on how well such measures match what the attackers are trying to do. Blast hardening that makes a target more difficult to damage with explosives will perform its intended function whether or not the security guards of the facility know a bomb has been planted. But if the measure does not match the threat, it will not help. Blast hardening in a subway system will not affect the chances of a successful chemical or incendiary attack because it is not matched to either of those threats, but a water sprinkler system might if it were designed such that it could both put out fires created by the incendiaries and help decontaminate after the chemical release.[58] How good the match is depends on how much the measures can reduce an attack's effects; e.g., robust blast hardening may make very small bombs irrelevant at some targets (essentially a 100 percent match between measure and threat) but only partially reduce the damage from larger devices (a less complete match).[59]

For measures that require that the terrorists' be detected first, how well they match is determined both by detection capability (discussed above) *and* the ability to successfully act once the threat is detected. Affecting the chances a terrorist plot will be successful requires both.[60] Awareness without the ability to act (or awareness without successful recognition of the threat)[61] does not increase the attackers' chance of failure.[62] This applies both to intelligence and law enforcement efforts to disrupt attacks before they are initiated and many protective measures at potential targets (e.g., detection technologies covering a target supported by a guard force that can act when the alarms go off).[63]

[58] A straightforward example of this match-mismatch dynamic is the security barrier being used by Israel to deny access to suicide bombers. Such a perimeter can be used to control the flow of people and is therefore well matched to such ground-based threats. In contrast, it does nothing against rockets fired by Palestinian groups over the barrier into Israel. Those weapons have been selected by the groups (and their use increased) precisely because of the mismatch between the weapons and that particular security measure, which has denied them in large part the use of more-effective suicide bombing operations. Taking matches and mismatches into consideration is also relevant in planning for many preparatory measures for biological threats; for example, for vaccines to have a beneficial protective effect, they must match the agent that is actually used in a subsequent attack.

[59] See, for example, National Academies (1995) for a discussion of blast hardening, its application to terrorism prevention at potential targets, and the matching of the protection to particular threats.

[60] See, for example, our work looking at metrics for understanding the effectiveness of domestic intelligence activities for counterterrorism (Jackson, 2009).

[61] For example, the questions raised whether MI5 in the United Kingdom was aware of one or more of the bombers that staged the July 7, 2005, attacks on the London Underground as a result of the earlier Operation Crevice investigation (Times Online, 2007).

[62] For example, Palmer (1995, p. 294) relates the story of a 1982 Sendero Luminoso operation, its first major urban attack, where good intelligence of the attack was received but "the local commander did not take the intelligence seriously, so only four guards were on duty at the prison when the attack came. The reinforcements were asleep in the police barracks a dozen blocks away, where they were completely pinned down by a supplementary Sendero force." In contrast, in the Homeland Security Institute analysis, whether the security organizations were aware of the terrorists was viewed as a stand-alone factor as a driver of failure (Homeland Security Institute, 2007, p. 99).

[63] For example, Kaplan and Kress (2005) performed a theoretical study on the potential effectiveness of even very-high-probability suicide-bomber detection being translated into reductions in casualties: Because of limited responses, the casualty reduction from detection was less than might be assumed a priori. The discussions of levels of operative skills with respect to attackers in Hoffman (1985) are similarly relevant for considering the potential effectiveness of security forces protecting potential targets.

Assuming an operation is detected, how should we think about the match between the security measures and the planned operation? As was the case for the blast-hardening example above, how well they are matched depends on what effect they can have on the attack's outcomes. Quick and effective action when an attack is detected can disrupt it such that it fails completely, e.g., bomb technicians defusing a planted bomb.[64] Routine success in achieving such an outcome would demonstrate a high degree of match between security efforts and the threat. In some cases, however, the best that a security or protective measure will be able to achieve will be to reduce the effects of the attack; for example, guards preventing a suicide bomber from approaching close to his target before detonation but being unable to stop the attack entirely. In such cases the match between security efforts and the threat is less complete.[65]

As was the case on the terrorist side of the interaction, our discussion of security measures has been intentionally static. At issue is the degree of match between security and protective measures and terrorist capabilities/plans at the time an attack is underway. However, in a conflict that persists over a longer time period, potentially with multiple interactions between the attacker and security/defensive measures, there can be dynamic change on the security side as well. Improvements in technologies or intelligence efforts might increase the chance of a particular type of plot being detected. Additional hardening at particular targets of concern or adjustments in other security measures might greatly increase the match between protective efforts and terrorist attacks that might be staged in the future. As a result, just as innovation on the adversary side can make terrorism a "moving target" for defenders, innovation on the part of the defense creates the same dynamic for the attacker.

This match and mismatch dynamic regarding security or protective measures and terrorist chances of success—where in this case mismatch is good for the attacker—creates the potential for trades that can shape terrorist planning and operational preferences. If the attackers are aware of particular security measures, their views about their capabilities can translate into additional requirements (i.e., the need for more information, technology, human resources, or higher/different skill levels) in the attackers' effort to lessen the chance that security or protective measures will affect their chance of operational success.

In our framework, this could be viewed as the attacker trying to pull the "security and protection" rings illustrated in the Venn diagrams in Figure 1 away from either the group ring or the operational ring to create mismatch where there might initially have been a match. For example, a group selecting a different weapon to strike a protected target (e.g., a mortar instead of a placed bomb) would be a technological approach to increase the mismatch between the security and the operation and reduce the chance it would be effective in stopping it. The group simply changing what it wanted to do by picking a different target—one without protection—would be another route to the same end. A group honing its operational skills to better conceal members already suspect of being threats by police forces is another example. Such activities

[64] The effectiveness of guard forces for different types of threats depends on their implementation and can be shaped by many variables. See Sagan (2004) for a discussion of some effectiveness challenges particular to such human security systems.

[65] Note that there may be tradeoffs between the degree of match of security or protective measures for a given attack type and those measures may have general utility across many attacks. If the price of a high level of matching for one sort of attack is that the measure has no effect on all other terrorist threats, that price may be too high given the uncertainty about the specific terrorist threats that will manifest in the future.

reflect attackers either seeking to create mismatches by avoiding security measures or by overmatching them[66] by adding resources to their attack operation.[67] These strategies represent an interaction between the security or protective measures. Just as in our discussion of how an attacker's views of the skill and capability requirements could produce additional steps or resource requirements they would need to fulfill before staging the attack, an attacker seeking to put these strategies in practice might create other signatures that might betray its efforts to intelligence or law enforcement, push up the resource requirements of an attack beyond what the group can tolerate, and so on.

Factors Outside the Attackers' Control. In considering the three main elements of our framework and the matches or mismatches between them, we have focused on characteristics where an attacker has some control over the factors that contribute to the success and failure of a potential attack. But in thinking about what causes the success or failure of terrorist attacks, there are also factors that are simply outside the control of the attackers.[68] For a pending terrorist operation, a myriad of things could happen that would increase the chances the attack will not be successful.[69] A traffic accident on a road critical to the attack could stop it in its tracks. A freak storm could cause the cancellation of the outdoor concert the group was targeting. A key operative gets sick. And so on. In some cases, such events will simply postpone the operation, but in others they will mean it cannot be staged at all.

Although such factors almost by definition cannot be integrated into the type of framework we are discussing here—both because their effect cannot be generalized and because their occurrence should not be a cornerstone of security planning—they cannot be ignored either. Some generalizations can be drawn based on the characteristics of different operations. Some attacks rely for their success on events that the attackers do not directly control. A kidnapping that relies on the target traveling to work along one of many possible routes is more likely to have problems than one for a target that has only one possible road to travel.[70] Intelligence or habitual behavior by the target may narrow the likely paths, but it cannot remove this dependence in the operation on something the attackers cannot directly control. Operations with many such elements are more likely to break down than ones with fewer, but once put into play, their net effect on a specific operation is difficult to project. This irreducible element of chance provides a fitting and appropriate caveat: Because even the most systematic effort to think through why operations succeed or fail cannot capture everything, the results of such efforts should be viewed as seeking to *anticipate* rather than *predict* groups' likely success or failure in future operations, though doing so can still help in best allocating scarce defensive resources.

[66] Combining concepts discussed here with those discussed under group planning skills in an examination of a historical dataset of force-on-force attacks by non-state groups, Meyer et al. (1993) concluded that in most cases groups chose a target whose security force they could readily overcome.

[67] See additional examples in our previous work on terrorist responses to defensive measures (Jackson et al., 2007).

[68] See, for example, discussion of randomness in the outcome of assassination attempts in Jones and Olken, 2007.

[69] See, for example, discussion in Levi (2007, p. 8) of "Murphy's Law of [in his case] Nuclear Terrorism: What can go wrong, might go wrong."

[70] A historical example of a group having such a problem was the assassination of Tsar Alexander II by Narodnya Volya, which had to improvise in their operational design when he changed his route at the last minute (Clutterbuck 2004, p. 171).

Conclusions: Matches and Mismatches for Security Planning

In trying to understand or anticipate the likelihood of the success or failure of potential terrorist operations, we have found the concept of matches and mismatches between classes of characteristics to be a useful way of breaking a complex problem into more understandable pieces. As a result, it provides something that has been missing in previous treatments of this problem: a means to move beyond lists of factors to a framework to think through more-general security problems in a systematic way. In applying these concepts to think through security problems, we see several areas of particular value:

- First, organizing thinking in this manner gets beyond analyzing factors in isolation to focus on key *relationships*, and in many cases, it is the nature of the relationship—rather than the absolute values of any of the factors—that truly contributes to a terrorist attack going as its authors planned. This is important for developing accurate threat assessment because focusing on the factors rather than relationships could lead to either artificially high or low assessments of the threat posed by the group.

- Second, focusing on these sets of matches and mismatches provides a more systematic way of thinking about how different classes of security measures align or do not align to different types of threats. The search for certain mismatches between protective measures and possible attack operations is traditional vulnerability-based threat assessment, but combining thinking about how a specific attack team might or might not overmatch a guard force of known capability with how well passive measures do or do not match those same threats provides a more integrated approach to protective planning.

  Similarly, looking at how security efforts either do or do not align with groups of varied characteristics is a different way of thinking about surveillance or intelligence planning. While being prepared to capitalize on group operational security mistakes is important, considering how changes in security measures might create new matches that benefit the defense is a more proactive strategy. For example, if changes in the security around a high-profile target sufficiently increase the operational security requirements for pre-attack surveillance, that mismatch may mean future attackers will be forced to attack without enough information to stage a consequential operation.

- Third, identifiing mismatches between a group's capabilities and what is known about its intentions may also provide clues to security organizations as to what activities to watch for in the future. A significant mismatch (if it has been recognized by the group) would suggest the need for more pre-attack preparation on the terrorists' part to reduce the shortfall, potentially creating additional opportunities to detect and disrupt their activities. The more a group stays within its comfort zone and only seeks to stage operations that are well within its capabilities, the less pre-attack preparation would likely be required and the quicker it could stage operations; therefore, there would likely be fewer opportunities for intervention.

  In these potential differences among groups—between groups seeking to carry out operations well within their capabilities versus those that are reaching beyond what they can currently achieve—we see as an additional reason to draw a distinction between *characteristics* (e.g., a group's operational skills) and the *processes* that can affect them

> when considering why operations succeed and fail. Beyond just avoiding the potential for double counting during an analysis of why an operation might succeed or fail, mixing the two could result in intelligence efforts missing an opportunity (e.g., recognizing the need for particular types of training by a group and therefore focusing attention on detecting it) or underestimating the threat posed by a group that has not been observed carrying out a process that it does not, in fact, need to stage successful future attacks.

These strengths lead us to conclude that focusing attention on a small set of practical relationships in this manner—how different characteristics do or do not match one another—could help to guide analysis of why past terrorist operations went as they did, and, more importantly, could help to identify opportunities to shape the chance of success or failure of future operations.

References

Abrams, Max, “Why Terrorism Does Not Work,” *International Security*, Vol. 31, No. 2, 2006, pp. 42–78.

Ahmed, Fazal, “Terrorism as a Rational Tactic: An International Study,” Ph.D. dissertation, Public Policy and Management, University of Pennsylvania, 1998.

Aid, Matthew M., “All Glory is Fleeting: SIGINT and the Fight Against Terrorism,” *Intelligence and National Security*, Vol. 18, No. 4, 2003, pp. 72–120.

Atran, Scott, “The Moral Logic and Growth of Suicide Terrorism,” *The Washington Quarterly*, Vol. 29, No. 2, 2006, pp. 127–147.

BBCNews, “Madrid Attacks Timeline,” March 12, 2004a. As of March 24, 2009:
http://news.bbc.co.uk/2/hi/europe/3504912.stm

———, “Timeline: Madrid Investigation,” April 28, 2004b. As of March 24, 2009:
http://news.bbc.co.uk/2/hi/europe/3597885.stm

Bell, J. Bowyer, “Conditions Making for Success and Failure of Denial and Deception: Nonstate and Illicit Actors,” *Trends in Organized Crime*, Vol. 6, No. 1, 2000, pp. 32–61.

———, *Assassin: Theory and Practice of Political Violence*, New Brunswick, N.J.: Transaction Publishers, 2006.

Benmelech, Efraim, and Claude Berrebi, “Attack Assignments in Terror Organizations and The Productivity of Suicide Bombers,” Cambridge, Mass.: Department of Economics, Harvard University, n.d. As of March 14, 2009:
http://www.economics.harvard.edu/faculty/benmelech/files/Terror_NBER_0207.pdf

Brachman, Jarret M., and William F. McCants, “Stealing Al Qaeda’s Playbook,” *Studies in Conflict & Terrorism*, Vol. 29, 2006, pp. 309–321.

Burton, Fred, “Beware of ‘Kramer’: Tradecraft and the New Jihadists,” stratfor.com, January 19, 2006. As of March 24, 2009:
http://www.stratfor.com/beware_kramer_tradecraft_and_new_jihadists

Canadian Security Intelligence Service, “Irish Nationalist Terrorism Outside Ireland: Out-of-Theatre Operations 1972–1993,” 1994. As of January 20, 2005:
http://www.csis-scrs.gc.ca/pblctns/cmmntr/cm40-eng.asp

Clutterbuck, Lindsay, “The Progenitors of Terrorism: Russian Revolutionaries or Extreme Irish Republicans?” *Terrorism and Political Violence*, Vol. 16, No. 1, 2004, pp. 154–181.

Coogan, Tim Pat, *The IRA: A History*, Niwot, Colo.: Roberts Rinehart, 1993.

Cragin, Kim, “Hizballah, the Party of God,” in Jackson et al., 2005.

Cragin, Kim and Sara A. Daly, *The Dynamic Terrorist Threat: An Assessment of Group Motivations and Capabilities in a Changing World*, Santa Monica, Calif.: RAND Corporation, MR-1782-AF, 2004. As of July 15, 2009:
http://www.rand.org/pubs/monograph_reports/MR1782/

Davis, Miriam, et al., *Dispensing Medical Countermeasures for Public Health Emergencies: Workshop Summary*, Washington, DC: National Academies Press, 2008.

della Porta, Donatella, "Left-Wing Terrorism in Italy," in Martha Crenshaw, ed., *Terrorism in Context*, University Park, Pa.: Pennsylvania State University Press, 1995, pp. 160–210.

Department of Energy, Office of the Inspector General, "Review of the Department of Energy's Canine Program at Selected Sites," DOE/IG-0755, January 2007.

DeRosa, Mary, "Data Mining and Data Analysis for Counterterrorism," Center for Strategic and International Studies, March 2004.

Dolnik, Adam, *Understanding Terrorist Innovation: Technology, Tactics, and Global Trends*, London: Routledge, 2007.

Don, Bruce W., David R. Frelinger, Scott Gerwehr, Eric Landree, and Brian A. Jackson, *Network Technologies for Networked Terrorists: Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations*, Santa Monica, Calif.: RAND Corporation, TR-454-DHS, 2007. As of July 15, 2009:
http://www.rand.org/pubs/technical_reports/TR454/

Drake, C. J. M., *Terrorists' Target Selection*, New York: St. Martin's Press, Inc., 1998.

Ellingwood, Ken, and Tracy Wilkinson, "Drug cartels' new weaponry means war," *Los Angeles Times*, March 15, 2009.

Enders, Walter, and Xuejuan Su, "Rational Terrorists and Optimal Network Structure," *Journal of Conflict Resolution*, Vol. 51, No. 1, 2007, pp. 33–57.

Fein, Robert A., and Bryan Vossekuil, "Assassination in the United States: An Operational Study of Recent Assassins, Attackers, and Near-Lethal Approachers," *Journal of Forensic Sciences*, Vol. 44, No. 2, 1999, pp. 321–333.

Forero, Juan, "Explosions Rattle Colombian Capital During Inaugural," *New York Times*, August 8, 2002.

Forrest, James M., *The Making of a Terrorist: Recruitment, Training, and Root Causes*, *Volume 2: Training*, Santa Barbara, Calif.: Praeger Security International, 2005.

Frank, Thomas, "Most Fake Bombs Missed by Screeners," *USA Today*, October 17, 2007, p. 1A.

Goldberg, Jeffery, "The Things He Carried," *The Atlantic*, November 2008.

Government Accountability Office, "Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public," GAO-06-1031, September 2006.

Heinzen, Karl, "Murder," *Die Evolution* (Biel, February–March, 1849), translated in Laqueur, Walter, ed., *Voices of Terror*, London: Reed Press, 2005, pp. 57–67

Hoffman, Bruce, *Commando Raids: 1946–1983*, Santa Monica, Calif.: RAND Corporation, N-316-USDP, 1985. As of July 15, 2009:
http://www.rand.org/pubs/notes/N2316/

———,"The Modern Terrorist Mindset: Tactics, Targets and Technologies," working paper, Centre for the Study of Terrorism and Political Violence, St. Andrews University, Scotland, October 1997. As of April 21, 2009:
http://www.ciaonet.org/wps/hob03/

Homeland Security Institute, "Underlying Reasons for Success and Failure of Terrorist Attacks: Selected Case Studies," June 4, 2007. As of March 8, 2009:
http://www.homelandsecurity.org/hsireports/reasons_for_terrorist_success_failure.pdf

Ilardi, Gaetano Joe, "Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control," *International Journal of Intelligence and CounterIntelligence*, Vol. 22, No. 2, 2009, pp. 246–274.

Jackson, Brian A., *Aptitude for Destruction, Volume 1: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism,* Santa Monica, Calif.: RAND Corporation, 2005a.

———,"Provisional Irish Republican Army," in Jackson et al., 2005b, pp. 93–140.

———, "Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and Its Application to Al Qaeda" *Studies in Conflict & Terrorism*, Vol. 29, No. 3, 2006, pp. 241–262.

———, “Counterinsurgency Intelligence in a ‘Long War’: Learning Lessons from the British Experience in Northern Ireland,” *Military Review*, Jan–Feb 2007, pp. 74–85.

———, “Exploring Measures of Effectiveness for Domestic Intelligence: Addressing Questions of Capability and Acceptability” in Brian A. Jackson, ed., *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency,* Santa Monica, Calif.: RAND Corporation, MG-804-DHS, 2009, pp. 179–204.
http://www.rand.org/pubs/monographs/MG804/

Jackson, Brian A., and David R. Frelinger, “Rifling Through the Terrorists’ Arsenal: Exploring Groups’ Weapons Choices and Technology Strategies,” *Studies in Conflict & Terrorism*, Vol. 26, No. 7, 2008, pp. 583–604.

———, “Emerging Threats and Security Planning: How Should We Decide What Hypothetical Threats to Worry About?” Santa Monica, Calif.: RAND Corporation, 2009. As of July 15, 2009
http://www.rand.org/pubs/occasional_papers/OP256/

Jackson, Brian A., David R. Frelinger, Michael J. Lostumbo, and Robert W. Button, *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles*, Santa Monica, Calif.: RAND Corporation, MG-626-DTRA, 2008. As of July 15, 2009:
http://www.rand.org/pubs/monographs/MG626/

Jackson, Brian A., Peter Chalk, Kim Cragin, Bruce Newsome, John V. Parachini, William Rosenau, Erin M. Simpson, Melanie W. Sisson, and Donald Temple, *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, Santa Monica, Calif.: RAND Corporation, MG-481-DHS, 2007. As of July 15, 2009:
http://www.rand.org/pubs/monographs/MG481/

Jackson, Brian A., John C. Baker, Peter Chalk, Kim Cragin, John V. Parachini, and Horacio R. Trujillo, *Aptitude for Destruction, Volume 2: Case Studies of Organizational Learning in Five Terrorist Groups*, Santa Monica, Calif.: RAND Corporation, MG-332-NIJ, 2005. As of July 15, 2009:
http://www.rand.org/pubs/monographs/MG332/

Jenkins, Brian Michael, *Embassies Under Siege: A Review of 48 Embassy Takeovers, 1971-1980*, Santa Monica, Calif.: RAND Corporation, R-2651-RC, 1981. As of July 15, 2009:
http://www.rand.org/pubs/reports/R2651/

———, “Safeguarding the Skies,” commentary, *San Diego Union Tribune*, September 30, 2001.

Jenkins, Brian Michael, and Bruce R. Butterworth, “Selective Screening of Rail Passengers,” MTI Report 06–07, February 2007.

Jenkins, Brian Michael, Janera Johnson, and David Ronfeldt, *Numbered Lives: Some Statistical Observations from 77 International Hostage Episodes*, Santa Monica, Calif.: RAND Corporation, P-5905, 1977. As of July 15, 2009:
http://www.rand.org/pubs/papers/P5905/

Jewkes, Yvonne, “Policing Cybercrime” in Tim Newburn, ed., *Handbook of Policing*, Devon, UK: Willan Publishing, 2003, pp. 501–524.

Jonas, Jeff, and Jim Harper, “Effective Counterterrorism and the Limited Role of Predictive Data Mining,” CATO Institue, Policy Analysis No. 584, December 11, 2006.

Jones, Benjamin F., and Benjamin A. Olken, “Hit or Miss? The Effect of Assassinations on Institutions and War,” Bureau for Research and Economic Analysis of Development, BREAD Working Paper No. 150, May 2007. As of March 17, 2009
http://ipl.econ.duke.edu/bread/papers/working/150.pdf

Jones, Calvert, “Al-Qaeda’s Innovative Improvisers: Learning in a Diffuse Transnational Network,” *Cambridge Review of International Affairs*, Vol. 19, No. 4, 2006, pp. 555–569.

Kaplan, Edward H., and Moshe Kress, “Operational effectiveness of suicide-bomber-detector schemes: A best-case analysis,” *Proceedings of the National Academy of Sciences*, Vol. 102, No. 29, 2005, pp. 10399–10404.

Kendig. J. C., Jr., and A. W. Zumpetta, “Police Handgun Dilemma: Revolver vs. Semi-Auto,” *Law and Order,* Vol. 39, No. 8, August 1991, pp. 93–96.

Kirby, Aidan, "The London Bombers as "Self-Starters": A Case Study in Indigenous Radicalization and the Emergence of Autonomous Cliques," *Studies in Conflict & Terrorism*, Vol. 30, No. 5, 2007, pp. 415–428.

Kutz , Gregory D., and John W. Cooney, "Aviation Security: Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process," Government Accountability Office, GAO-08-48T, November 15, 2007.

Kydd, Andrew H., and Barbara F. Walter, "The Strategies of Terrorism," *International Security*, Vol. 31, No. 1, Summer 2006, pp. 49–80.

Levi, Michael, *On Nuclear Terrorism*, Cambridge, Mass.: Harvard University Press, 2007.

McCormick, Gordon H., "Terrorist Decision Making," *Annual Review of Political Science,* Vol. 6, No. 1, 2003, pp. 498–499.

McGartland, Martin, *Fifty Dead Men Walking*, London: Blake Publishing, 1997.

Meyer, Christina, Jennifer Duncan, and Bruce Hoffman, *Force-on-Force Attacks: Their Implications for the Defense of U.S. Nuclear Facilities*, Santa Monica, Calif.: RAND Corporation, N-3638-DOE, 1993. As of July 15, 2009:
http://www.rand.org/pubs/notes/N3638/

Miller, Martin A., "The Intellectual Origins of Modern Terrorism in Europe," in Martha Crenshaw, ed., *Terrorism in Context*, University Park, Pa.: Pennsylvania State University Press, 1995, pp. 27–62.

Moghadam, Assaf, "Suicide Terrorism, Occupation, and the Globalization of Martyrdom: A Critique of Dying to Win," *Studies in Conflict and Terrorism*, Vol. 29, 2006, pp. 707–729.

National Academies, *Protecting Buildings from Bomb Damage: Transfer of Blast-Effects Mitigation Technologies from Military to Civilian Applications,* Washington, D.C.: National Academies Press, 1995.

———, *Existing and Potential Standoff Explosives Detection Techniques,* Washington, D.C.: National Academies Press, 2004.

———, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment,* Washington, D.C.: National Academies Press, 2008.

National Commission on Terrorist Attacks on the United States, *The 9/11 Commission Report*, 2004.

Oots, Kent Layne, *A Political Organization Approach to Transnational Terrorism*, New York: Greenwood Press, 1986.

Palmer, David Scott, "The Revolutionary Terrorism of Peru's Shining Path," in Martha Crenshaw, ed., *Terrorism in Context*, University Park, Pa.: Pennsylvania State University Press, 1995, pp. 249–308.

Pape, Robert A., "The Strategic Logic of Suicide Terrorism," *American Political Science Review*, Vol. 97, No. 3, 2003, pp. 1–19.

Parachini, John V., "Aum Shinrikyo," in Jackson et al., 2005, pp. 11–35.

Pedahzur, Ami, Arie Perliger, and Leonard Weinberg, "Altruism and Fatalism: The Characteristics of Palestinian Suicide Terrorists," *Deviant Behavior: An Interdisciplinary Journal*, Vol. 24, 2003, pp. 405–423.

Phillips, Peter J., "The 'Price' of Terrorism," *Defence and Peace Economics,* Vol. 16, No. 6, 2005, pp. 403–414.

Quillen, Chris, "A Historical Analysis of Mass Casualty Bombers," *Studies in Conflict & Terrorism*, Vol. 25, 2002, pp. 279–292.

Rabasa, Angel, Robert D. Blackwill, Peter Chalk, Kim Cragin, C. Christine Fair, Brian A. Jackson, Brian Michael Jenkins, Seth G. Jones, Nathaniel Shestak, Ashley J. Tellis, *The Lessons of Mumbai*, Santa Monica, Calif.: RAND Corporation, OP-249-RC, 2009. As of July 15, 2009:
http://www.rand.org/pubs/occasional_papers/OP249/

Rapoport, David C., *Assassination and Terrorism*, Toronto: Canadian Broadcasting Corporation, 1971.

Roggio, Bill, "Pakistani Forces Thwart Triple Suicide Bombing Attack," longwarjournal.org, August 29, 2008. As of March 24, 2009:
http://www.longwarjournal.org/archives/2008/08/pakistani_forces_thw.php

Sandler, Todd, and John L. Scott, "Terrorist Success in Hostage-Taking Incidents: An Empirical Study," *Journal of Conflict Resolution*, Vol. 31, No. 1, 1987, pp. 35–53.

Sagan, Scott S., "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security," *Risk Analysis*, Vol. 24, No. 4, 2004, pp. 935–946.

Shapiro, Jacob N., "The Terrorist's Challenge: Security, Efficiency, Control," Center for International Security and Cooperation, Stanford University, April 26, 2007. As of March 24, 2009:
http://igcc.ucsd.edu/pdf/Shapiro.pdf

Sharif, Idris, *The Success of Political Terrorist Events: An Analysis of Terrorist Tactics and Victim Characteristics, 1968–1977*, Lanham, Md.: University Press of America, 1996.

Silke, Andrew, "Beyond Horror: Terrorist Atrocity and the Search for Understanding—The Case of the Shankill Bombing," *Studies in Conflict & Terrorism*, Vol. 26, No. 1, 2003, pp. 37–60.

Strinkowski, Nicholas Charles, *The Organizational Behavior of Revolutionary Groups*, Evanston, Ill.: Northwestern University, 1985.

Technology and Privacy Advisory Committee, "Safeguarding Privacy in the Fight Against Terrorism," U.S. Department of Defense, March 2004.

Times Online, "MI5 Criticised for Missing 7/7 Link to Operation Crevice," April 30, 2007. As of March 24, 2009: http://www.timesonline.co.uk/tol/news/uk/article1726161.ece

Vick, Alan, *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases*, Santa Monica, Calif.: RAND Corporation, MR-553-AF, 1995. As of July 15, 2009:
http://www.rand.org/pubs/monograph_reports/MR553/

Wein, Lawrence M., and Yifan Liu, "Analyzing a bioterror attack on the food supply: The case of botulinum toxin in milk," *Proceedings of the National Academy of Sciences,* Vol. 102, No. 28, 2005, pp. 9984–9989.