CAN WE DETER TERRORISTS FROM EMPLOYING WEAPONS OF MASS DESTRUCTION ON THE U.S. HOMELAND?

Colonel Gordon Drake,
United States Army

Group Captain Warrick Paddon,
Royal Australian Air Force

Lieutenant Colonel Daniel Ciechanowski,
United States Air Force

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
07-04-2003		xx-xx-2002 to xx-xx-2003

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Can We Deter Terrorists From Employing Weapons of Mass Destruction on the U.S. Homeland? Unclassified	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)	5d. PROJECT NUMBER
Drake, Gordon ; Author	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College Carlisle Barracks Carlisle, PA17013-5050	

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS	10. SPONSOR/MONITOR'S ACRONYM(S)
,	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 78	19. NAME OF RESPONSIBLE PERSON Rife, Dave RifeD@awc.carlisle.army.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number DSN

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39.18

DISCLAIMER

The views expressed in this academic research paper are those of the authors and do not necessarily reflect the official policy or position of the United States Government, the United States Department of Defense, any of its agencies, or the Royal Australian Air Force. In accordance with Air Force Instruction 51-303, it is not copyrighted but is the property of the United States and Australian Governments.

iii

ABSTRACT

Information discovered as a result of the current war on terrorism suggests a terrorist-led attack on the U.S. homeland involving weapons of mass destruction (WMD) remains a very real possibility. Some believe the U.S. faces its greatest WMD threat since the 1962 Cuban missile crisis, but many discount the effect deterrence can have on terrorist groups. Deterrence, however, is an attractive option in that the costs to implement a deterrence-based strategy are minimal when compared to defending the entire homeland or defeating all elements of a threatening terrorist organization. Little research, however, has been done to evaluate the effectiveness deterrence can have on a group bent on harming the U.S. with WMD.

This paper attempts to fill this void in the literature by exploring the contributions deterrent strategies can have on a terrorist group who may have the capability and/or intent to launch a WMD attack on America. A four-step model comprising 1) Screening, 2) Analyzing, 3) Strategizing, and 4) Monitoring is developed to serve as a framework for policymakers in determining how to allocate resources and effort among deter, defend, and defeat strategies. At each step, the model uses predictive organizational and self-examination factors to highlight the adversary's vulnerabilities and outline potential deterrent strategies. It is then tested against al Qaeda, the terrorist organization presently posing the most likely WMD threat to the U.S. homeland, in order to demonstrate its utility. The paper concludes with significant findings and recommendations for action.

ACKNOWLEDGMENTS

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

x

EXECUTIVE SUMMARY

Thesis Question: To what extent can the U.S. rely on deterrence as a means of protection against a WMD attack on the U.S. homeland?

Information discovered during the current War on Terrorism (WOT) suggests a terrorist-led weapons of mass destruction (WMD) attack against the U.S. homeland remains a very real possibility. Some believe this means the U.S. faces its greatest WMD threat since the 1962 Cuban Missile Crisis; yet many discount deterrence as a means to combat this threat, since conventional wisdom holds that fanatical terrorist organizations are undeterrable. Deterrence is attractive, however, when compared to defend and defeat strategies because it is cost effective. In our opinion, relying completely on defeat and defend strategies unnecessarily reduces our ability to provide reasonable security by discounting a potentially effective strategy.

We cannot rely on even the best defend and defeat strategies to mitigate the adverse consequences of a determined WMD attack. Clearly, resolving the question of how well we can deter non-state actors from employing WMD on the U.S. homeland is both urgent and important.

In this paper we have developed a model policymakers can use to determine the degree to which terrorist organizations might respond to deterrence-based strategies. While every application will be different, when applying this model, policymakers will not only gain confidence in the appropriate Deter/Defend/Defeat balance, but will also obtain a clearer understanding of the organization's potential vulnerabilities.

Our Screen-Analyze-Strategize-Monitor (SASM) model involves a four-step process below:

- **Step 1: SCREEN** terrorist organizations to see if they pose any WMD threat to the U.S. homeland.

- **Step 2: ANALYZE** details of organizational traits to reveal potential vulnerabilities that may suggest deterrence will be successful.

- **Step 3: STRATEGIZE** by identifying the terrorist organization's vulnerabilities, assessing the U.S.'s potential to target those vulnerabilities (alone or with assistance), and then implementing a deterrence plan tailored to the specific WMD threat.

- **Step 4: MONITOR** to determine any weakness or achieved success and to provide feedback so that the deterrence plan can be adjusted or abandoned.

To test the utility of the SASM model, we ran the model against the one terrorist organization appearing to have both the intent and the capability to conduct a WMD attack on the U.S.: al Qaeda. In summary, our case study of the al Qaeda terrorist system reveals that, at the strategic level, senior leadership and ideologues are unlikely to be deterred from their purpose.   Accordingly, the U.S.'s principal response to this component of the organization should rely primarily on defend and defeat strategies.   However, we found that any states providing safe haven or technical support to al Qaeda might be responsive to deterrence.   At the operational and tactical levels of the organization, we arrive at a different conclusion. At these levels we have determined that considerable value may be obtained by targeting Arab benefactors, infiltrated charities and the tactical cells with a media campaign designed to expose the supporters and discredit al Qaeda's pseudo-Islamic ideology.

The al Qaeda case study validates the utility of employing the SASM model to evaluate potential WMD threats to the U.S. While conventional wisdom suggests terrorists cannot be deterred, our analysis convinces us that deterrence-based strategies are not given sufficient credit and can contribute to protecting the U.S. homeland from a WMD attack. Key findings and recommendations are outlined below.

Findings:

- Deterrence can play a significant role in preventing a WMD attack on the U.S. homeland.

- The SASM model presents policymakers with a structured framework with which to assess the feasibility of identifying measures that may serve to deter a terrorist WMD attack on the U.S. homeland.

- When contemplating deterrent-based strategies, it is essential to break the target terrorist network into its strategic, operational, and tactical levels

- Some components may be responsive to deterrent strategies while others within the organization may not.

- Deterring one or more critical components of a terrorist system at one level could be enough to deter the entire network.

- Defend, Defeat, and Deter strategies overlap to some extent and are mutually reinforcing.

- The SASM model provides the policymaker with a rigorous framework that can be used to evaluate deterrent-based strategies.

Recommendations:

We urge the NSC to direct the Department of Defense (DoD) to lead an interagency effort aimed at implementing the SASM methodology. While DoD is arguably best suited to lead this effort, the Department of State, the Department of Homeland Security, and the Intelligence Community should play major roles.

Furthermore, we recommend adding a fourth pillar entitled "Deterrence" to the "National Strategy to Combat Weapons of Mass Destruction" to reflect more accurately the value deterrence can bring to the war on terrorism.[1]

---

[1] *National Strategy to Combat Weapons of Mass Destruction*, Washington, D.C.: The White House, Dec. 2002: 1-6.

CHAPTER 1: THINKING ABOUT THE UNTHINKABLE

Imagine reading a headline proclaiming "3828 Dead, Over 30,100 Permanently Disabled or Injured, Some 173,000 Temporarily Injured in World's Worst Chemical Incident." Were this true, it would certainly grab national attention and induce panic and fear that would spread across the country like wildfire. The problem is, such an event did actually occur, and the headline could well have been written, because it describes the tragic outcome of a real-world catastrophe – the methyl isocyanate leak at Union Carbide's pesticide plant in Bhopal, India on December 3, 1984.[1] A terrorist chemical agent attack in this country yielding similar horrific mass casualties could significantly change our way of life.

Increasingly, it appears terrorists want to inflict this scale of mass casualties on the U.S. homeland and are considering weapons of mass destruction (WMD) to accomplish it.[2] In fact, it may be just a matter of luck that it has not happened yet. If, for argument's sake, we assume that the probability of a terrorist WMD attack against the U.S. is 10% per annum over each year of a 50-year period, there is a 99.49% chance it will happen at least once during that 50 years. Similarly, if we drop the likelihood to 3% per year, the probability over 50 years is still an unacceptable 21.8%.[3] In short, if we consider just the nuclear piece of WMD, "Could a nuclear terrorist attack happen today? Our considered answer is: yes, unquestionably, without any doubt. It is not only a possibility, but in fact the most urgent national security threat to both the United States and Russia."[4] The ramifications? "A half dozen nuclear explosions across the United States or Russia would shift the course of history."[5]

The September 11th (9/11) attacks, more deadly than all terrorist attacks against Americans in the previous 50 years combined, demonstrated that terrorism has shifted dramatically.[6] In the aftermath of these assaults, both the threat and the stakes are far greater than they have ever been. For the first time, the U.S. faces the risk of a no-warning WMD attack on its soil. Several experts in the field appear to share the view that "[t]he danger of weapons of mass destruction being used against America and its allies is greater now than at any time since the Cuban missile crisis of 1962"[7] and that "… NBC [nuclear, biological and chemical] terrorism poses one of the most serious national-security challenges of the modern era."[8] There is little doubt among these experts, for example, that a terrorist nuclear threat currently exists: once "they [terrorists] get their hands on the material, they'll have it [a nuclear device]."[9]

The U.S. requires an effective policy response to this challenge. The counterterrorism policy of the U.S. government includes deterrence of terrorism as enshrined in Presidential Decision Directive (PDD) 39, Subject: U.S. Policy on Counterterrorism, signed on June 21, 1995: "It is the policy of the United States to *deter*, defeat and respond vigorously to all terrorist attacks … [T]he U.S. shall pursue vigorously efforts to *deter* … individuals who perpetrate or plan to perpetrate such attacks (italics added)."[10] However, the overwhelming emphasis of discussion within both government and academia in trying to prevent a terrorist WMD attack from occurring on the U.S. homeland centers on what we call in this paper Defend and Defeat strategies. Most analysts seem to ignore deterrence by assuming it is not feasible.

We believe that until policymakers have analyzed in a systematic way those potential terrorist organizations that might use WMD, we should not reject deterrence out of hand. The Bush Administration explicitly recognizes the need for a comprehensive strategy in its December 2002 "National Strategy to Combat Weapons of Mass Destruction": "Weapons of mass destruction (WMD) – nuclear, biological, and chemical – in the possession of hostile states and terrorists represent one of the greatest security challenges facing the United States. We must pursue a comprehensive strategy to counter this threat in all of its dimensions."[11] While this document recognizes a role for deterrence of WMD within its counterproliferation pillar, we have advanced this concept one step further by creating a model that policymakers can use to realize that role. This paper provides the framework to operationalize a strategy of deterrence of a terrorist WMD attack against the U.S. homeland.

METHODOLOGY AND APPROACH

Our methodology includes a literature survey and personal interviews with prominent academics and policymakers in the fields of terrorism, WMD, and deterrence. While this research has been confined to unclassified sources, many of the practitioners interviewed had current access to relevant classified material. They have validated the approach we have pursued, so we are confident that our analysis is confined within reasonable boundaries of error. The centerpiece of the paper is a model that provides a framework to determine when deterrence might constitute an appropriate strategy to confront a terrorist organization that could use WMD against the U.S. homeland. Through the vehicle of the model, we capture deterrence-based strategies for policymakers and suggest some possible means to operationalize them.

Our model has four steps, which gives the framework its name – **S**creen, **A**nalyze, **S**trategize, and **M**onitor (SASM). Several high-level experts in the field[12] lead us to believe that providing a visual framework will be of utility to policymakers. Our intent is to capture processes that may already be used within government but are currently unstructured, undocumented, or uncoordinated. The aim is to give policymakers, who are busily putting out daily brushfires, the benefit of a structured operational approach.

In the following chapter, we will define the threat and the terms *deterrence*, *defend*, *defeat*, *WMD*, and *terrorism*. Chapter 3 outlines key assumptions and provides a detailed look at the SASM model, step-by-step, to illustrate where and when deterrence might work. In Chapter 4 we test the model with a real terrorist organization, al Qaeda, to validate its utility and understand its limits. We have selected al Qaeda because it is the one group that is clearly recognized as having intent and capability to use WMD against the U.S. Finally, in Chapter 5, we present our findings and advance some recommendations for policymakers so they can use the SASM model to advantage.

[1] See Bhopal: Chronology as of November 2002, 23 Jan. 2003, <http://www.bhopal.com/chrono.htm>.

[2] Jessica Stern, "Terrorist Motivations and Unconventional Weapons" in Peter R. Lavoy, Scott D. Sagan, and James J. Wirtz, ed, *Planning the Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons* (Ithaca, New York and London: Cornell University Press, 2000) 202.

[3] Graham Allison, "Preventing Nuclear Terrorism," MIT Center for International Studies Seminar, 292 Main St, Cambridge, Mass., 4 Dec. 2002.

[4] Graham Allison and Andrei Kokoshin, "The New Containment: An Alliance Against Nuclear Terrorism," *The National Interest* 69 (2002) 35.

[5] Allison and Kokoshin 36.

[6] Until 9/11, terrorists globally had killed no more than approximately 1000 Americans since 1968, the year credited with signifying the advent of modern, international terrorism. Bruce Hoffman, "Lessons of 9/11," Joint Inquiry Staff Request (Washington DC: RAND, 8 Oct. 2002) 7. The attacks of 9/11 killed almost 2900 citizens of the world.

[7] Ashton Carter, John Deutch, and Philip Zelikow, "Catastrophic Terrorism: Tackling the New Danger," *Foreign Affairs* 77.6 (1998) 81.

[8] Richard A. Falkenrath, "Confronting Nuclear, Biological and Chemical Terrorism," *Survival* 40.3 (1998) 44.

[9] Ashton B. Carter, personal interview, 26 Nov. 2002.

[10] *Presidential Decision Directive 39,* "U.S. Policy on Counterterrorism," Washington, D.C.: The White House, 21 Jun. 1995, <http://www.fas.org/irp/offdocs/pdd39.htm>.

[11] *National Strategy to Combat Weapons of Mass Destruction*, (Washington, D.C.: The White House, Dec. 2002) 1.

[12] Ashton Carter, Steven Miller, and Jessica Stern of Harvard University; Keith Payne of the U.S. Department of Defense; Kerry Kartchner of the U.S. Department of State; William McRaven of the U.S. National Security Council; and Bruce Hoffman and Paul Davis of RAND.

CHAPTER 2: DETERRENCE, TERRORISTS, AND WEAPONS OF MASS DESTRUCTION (WMD)

NEW TERRORISM

Today, we are confronted with a "new terrorism," which is a departure from the past in two fundamental respects: its leaders possess no moral compunction against using WMD or causing mass casualties, and both its leaders and followers are religiously and fanatically committed to die for a cause. "It [today's terrorism] seeks nothing less than a vast redistribution of global power and a geopolitical revolution that would end the hegemony of the United States and its Western allies."[1] The 9/11 attacks have shown terrorists how to harness the attributes of the 21st century – globalization, technology, instantaneous communications, the Internet, densely populated urban centers, and increasingly porous borders – to force grievances and demands upon a global audience compelled to listen while terrorists try to harm both the infrastructure and the psyche of the world's only remaining superpower. This new terrorism differs from the two principal forms of terrorism in the postwar era, national liberation and state-sponsored terrorism, which sought incremental change while avoiding wholesale killings. The older generation of terrorists sought political inclusion at a negotiating table, a goal that was inconsistent with atrocities. In contrast, the new terrorists aim to maximize death and destruction for its own sake as well as to sow mass panic and hysteria.

Terrorism expert Brian Jenkins' oft-quoted observation from 1975 – "Terrorists want a lot of people watching but not a lot of people dead"[2] – no longer applies to these new terrorists. Their increasing sophistication – synchronized attacks yielding exponentially more deaths and injuries – underlines the belief that they appear to harbor no constraints on inflicting mass casualties. RAND terrorism expert Bruce Hoffman attributes this fascination with mass casualties to the intense religious aspect of the new terrorism:

> Religious terrorism tends to be more lethal than secular terrorism because of the radically different value systems, mechanism of legitimization and justification, concepts of morality, and Manichean worldviews that directly affect the 'holy terrorists'' motivation. For the religious terrorist, violence first and foremost is a sacramental act or divine duty, executed in direct response to some theological demand or imperative and justified by scripture.[3]

In short, "The terrorists most likely to attempt to use WMD are groups with amorphous constituencies, including religious fanatics, groups that are seeking revenge and groups that are attracted to violence for its own sake."[4]

Theoretically, the type of terrorist group that would use WMD can be found where three terrorist organization subsets intersect: those who want to use WMD despite its formidable political costs, those who can acquire or develop them, and those who can deliver them covertly. While this intersection of groups is small today, it is growing.[5] Richard Falkenrath of Harvard University believes the WMD terrorism threat is increasing because the number of non-state actors that are both WMD-capable and desiring to cause mass casualties is growing.[6] Additionally, the terrorists' belief that they are engaged in a metaphysical battle changes the calculus used for the level of violence. Instead of committing carnage sparingly, they seek greater and more spectacular violence to fulfill divine commands.[7] The injection of a fervent religious belief can transform violence into a justifiable sacramental act, with the objective of accomplishing a religious goal before a divine judge while simultaneously meeting political demands.

DEFINITIONS

An understanding of the words deterrence, defend, defeat, WMD, and terrorism is key to effective implementation of the SASM model. While the current Department of Defense (DoD) definitions are useful departure points,[8] we will discuss them below and place them in a modern context.

Deterrence

The Department of Defense Dictionary of Military and Associated Terms defines deterrence in the following manner:

> The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction.[9]

While the threat of punishment is clearly a key ingredient of the term deterrence, other experts in the field define it more broadly. Glen H. Snyder, author of Defense and Deterrence, also includes denying the adversary the ability to achieve his war aims, and rewarding an enemy for refraining from taking undesirable actions. Snyder uses the following definition in his classic from 1961: "Essentially, deterrence means discouraging the enemy from taking military action by posing for him a prospect of

5

cost and risk outweighing his prospective gain."[10] Considering the terrorism paradigm the U.S. now faces, we believe the inclusion of threats of punishment, objective denial, and rewards are all important aspects of deterrence. These three elements are discussed below.

First, the classic Cold War threat of punishment remains pertinent and fundamental to any discussion of deterrence. Terrorists must be made to understand that they will pay a heavy cost should they choose to embark upon a WMD strategy. To the extent the U.S. can find targetable elements that a terrorist organization values, threatening their removal is one aspect of deterrence that must be pursued. According to Snyder:

> The objective of military deterrence is to reduce the probability of enemy military attacks, by posing for the enemy a sufficiently likely prospect that he will suffer a net loss as a result of the attack…[11]

Secondly, terrorist organizations do not like to take unmitigated risks. Convincing the adversary that proceeding down the path towards WMD employment is overly risky is another important aspect of any deterrent strategy. Snyder terms this element of deterrence denial:

> Denial capabilities—typically, conventional ground, sea and tactical air forces—deter chiefly by their effect on the fourth factor in the aggressor's calculus: his estimate of the probability of gaining his objective.[12]

While the U.S. will not primarily employ ground, sea, and tactical air forces to deny a terrorist organization the achievement of its goals, it should attempt to deny the group easy access to high technology and fissile material. To the extent the U.S. can convince the terrorist organization that obtaining these essential elements of a WMD program will be very difficult and risky, it has a chance to change the group's behavior and prevent a WMD event from occurring.

Finally, the most often forgotten aspect of deterrence involves rewards. While many may feel the concept of rewards does not fit within the definition of deterrence, Snyder feels it must be included. He writes:

> Deterrence, in one sense, is simply the negative aspect of political power; it is the power to dissuade as opposed to the power to coerce or compel. One deters another party from doing something by the implicit or explicit threat of applying some sanction if the forbidden act is performed, or by the promise of a reward if the act is not performed. Thus conceived, deterrence does not have to depend on military force.[13]

Many readers will cringe at the notion of using rewards to modify a terrorist organization's behavior, and we agree that rewarding terrorist groups across the board is bad policy. However, the concept

should not be dismissed out of hand. There may be some instances where rewards to elements of a terrorist system are appropriate and can help deter the overall organization from achieving its goals. For example, while it would clearly be inappropriate to reward bin Laden or his operatives for committing crimes against humanity, it might be appropriate to reward a potential state sponsor for securing its nation's fissile material. Likewise, it could be productive for the U.S. to hire a prospective WMD scientist away from bin Laden or address some social grievances in an area where al Qaeda recruits heavily in an attempt to undermine its base of support. Incentives can play a deterrent role and, if applied judiciously, might contribute to the overarching goal of deterring the organization from pursuing a WMD strategy.

Threats of punishment, objective denial, and rewards are the three key elements of our formulation of deterrence. Each must be considered when attempting to persuade a terrorist organization not to employ WMD on the U.S. homeland.[14]

Defend and Defeat Strategies

While our construct concerns itself with a deterrence strategy, it recognizes that there are three general U.S. strategies to keep terrorists from attacking the U.S. homeland with WMD: Defend, Deter, and Defeat. Defend and Defeat strategies have the advantage over those of Deter in that they provide highly visible and immediate responses.

Looking first at Defend strategies, full assurance is not possible – it would break the bank to safeguard against every potential terrorist WMD target in the U.S., and is not even feasible in the first place. Additionally, Defend strategies take a long time to implement. Time, like adequate funds, may not be available. Nevertheless, a Defend strategy will be continuously on-going as part of efforts to prevent a terrorist WMD attack. For example, airport and seaport security, increased surveillance along borders and at crossing points, and protecting key infrastructure such as nuclear reactors, high-visibility sporting and entertainment venues, and laboratories stocked with nuclear, biological, or chemical agents are essential to protect. The problem is that, given the magnitude of what has to be defended, complete defense is not feasible. Over 500 million people, 11 million trucks, two million rail cars, and 7500 foreign-flagged ships making 51,000 port calls enter the U.S. annually, not counting an unknown number of illegal entrants.[15]

Many, if not all, defensive activities serve a deterrent purpose if they dissuade a potential WMD terrorist from attacking a particular target with a certain means or even trying to import

components of a WMD weapon or the weapon in its entirety into the U.S. In fact, WMD experts such as Harvard's Ashton Carter, Philip Zelikow of the University of Virginia, and John Deutch at the Massachusetts Institute of Technology are emphatic that Defend measures are essential to a deterrence strategy, denying terrorists the opportunities to develop or acquire WMD by extending current prohibitions against WMD development or possession internationally because "[p]revention is intertwined with deterrence."[16] To the extent this occurs, some Defend measure can have a long-term deterrent effect.

At the other end of the spectrum, there may be cases when the only way to fend off a terrorist WMD attack is to defeat or eradicate the organization. While a strategy of defeating the organization in total is beyond the scope of this paper, deterrence can be served by certain Defeat actions. Near-term Defeat actions could have enduring deterrent impacts.

Defeat strategies are highly costly in two resource areas as well – funding and political capital. It could ultimately cost billions of dollars to pursue and eradicate WMD terrorists and their support infrastructure, which may include state sponsors. Additionally, for the U.S. to prosecute a full range of Defeat strategies, it would most likely have to expend substantial political capital as it seeks to employ all the elements of national power – political/diplomatic, economic/financial, military, informational, and legal – in ways that may well conflict with civil liberties at home and the preference of allies and friends for less aggressive response abroad. Deterrence, if successful, could prove to be far less disruptive than a strategy of defeat. In cases where deterrence could succeed, it could at least buy valuable time for policymakers to decide whether to continue with deterrence or transition to a Defeat strategy. As Barry Posen of the Massachusetts Institute of Technology observes:

> Particularly in the age of weapons of mass destruction, the United States cannot allow any state to participate in catastrophic attacks on its homeland with impunity. More intensive defensive precautions can reduce but not eliminate U.S. vulnerability to mass destruction attacks, so deterrence must be the first line of defense. For these reasons, the Taliban regime in Afghanistan had to be destroyed.[17]

Figure 1 on the next page illustrates our view of deterrence and the mutually reinforcing role Defend and Defeat actions can have on deterrence.
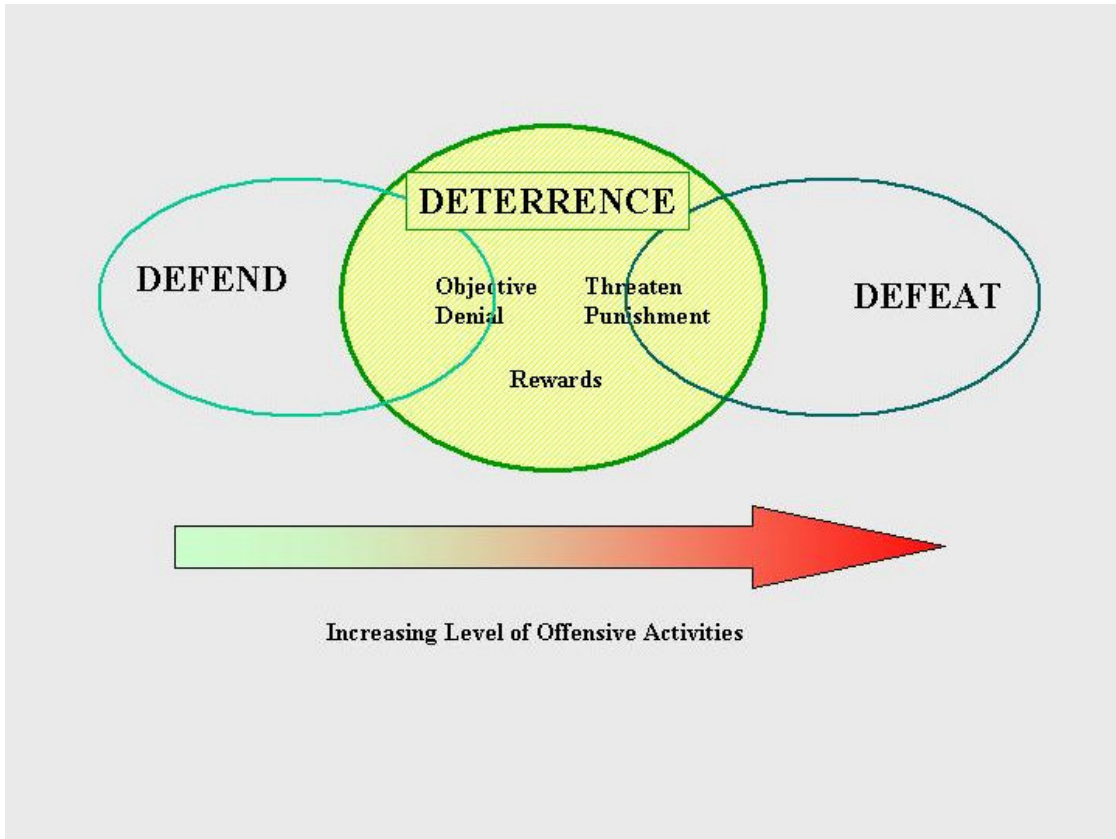
Figure 1: Mutually Reinforcing Strategies

WMD

We spent much time and effort settling on a term for the type of weapon and weapons effects we wanted to focus on in this paper. We decided on WMD for the following reasons: 1) the policy community seems to prefer WMD,[18] 2) the public understands this term better than the alternatives, 3) WMD captures the narrower focus of weapons important to us, as it represents the potential catastrophic effects on lives and property, and 4) the term imposes a firebreak between conventional weapons and special weapons that have the potential to yield catastrophic effects even beyond those experienced on 9/11.

While the type of weapon is important, we are also concerned about the potential for long-term effects, both physical and psychological. WMD are special and different from other potential mass casualty-producing weapons such as dirty bombs, enhanced high-yield explosives, and cyber attacks because they are invasive, entering the body invisibly to cause death, injury, and tremendous

fear. They can also destroy large areas of property or render it unusable for long periods of time.[19]
Thus, we require the fulfillment of all of the following criteria to meet our definition of WMD:

- potentially large-scale deaths (no specific number but at least a few thousand, on the order of 9/11)
- potential psychological scarring of individuals and masses, reinforcing a mass hysteria effect
- potentially permanent property devastation that would require inordinate time and money to clean up
- potentially wide and deep economic impact similar to but deeper than the aftermath of 9/11, estimated to be as high as three quarters of a percent of U.S. GDP or 75 billion dollars annually[20]
- changing the policies of the U.S. government away from the path the people want

We specifically exclude hijacked commercial aircraft as used on 9/11 as WMD because they did not use nuclear, biological, or chemical materials and therefore can be regarded as involving relatively bounded destructive effects.

Terrorism

For the purposes of this report, we adopt the RAND definition of terrorism: "violence committed or credibly threatened by groups in order to create fear and alarm within a population, either to cause a government to grant terrorists' demands or to otherwise achieve political objectives."[21]

Based on these concepts and definitions in Chapter 3, we present our framework for determining the impact deterrence can have on terrorist organization intent on employing WMD on the U.S. homeland. In doing so, we offer the policymaker a structured approach to a complex problem.

---

[1] Kurt M. Campbell and Michèle A. Flournoy, *To Prevail* (Washington, DC: The CSIS Press, 2001) 37.

[2] Brian M. Jenkins, "Will Terrorists Go Nuclear?" P-5541 (Santa Monica, Calif.: RAND, Nov. 1975) 4.

[3] Bruce Hoffman, "Lessons of 9/11," Joint Inquiry Staff Request (Washington DC: RAND, 8 Oct. 2002) 4.

[4] Jessica Stern, *The Ultimate Terrorists* (Cambridge, Mass.: Harvard University Press, 1999) 70.

[5] Jessica Stern, "Terrorist Motivations and Unconventional Weapons" in Peter R. Lavoy, Scott D. Sagan, and James J. Wirtz, ed, *Planning the Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons* (Ithaca, New York and London: Cornell University Press, 2000) 203.

[6] Richard A. Falkenrath, "Confronting Nuclear, Biological and Chemical Terrorism," *Survival* 40.3 (1998) 50.

[7] Campbell and Flournoy 39

[8] See Glossary for DoD definitions.

[9] *DoD Dictionary of Military and Associated Terms* 23 Jan. 2003, <http://www.dtic.mil/doctrine/jel/doddict/data/d/01643.html>.

[10] Glen H. Snyder, *Deterrence and Defense* (Princeton, New Jersey: Princeton University Press, 1961) 3.

[11] Snyder 12.

[12] Snyder 15.

[13] Snyder 9.

[14] In their monograph entitled "Deterrence and Influence in Counterterrorism," Davis and Jenkins define deterrence along traditional lines including threats of punishment and denial. External to deterrence, they add another term titled "influence," which entails additional measures including "co-optation" and "inducement." We have accepted a more broadly based definition by Snyder that includes "rewards" as part of deterrence. "Rewards," in our formulation, would be roughly synonymous with RAND's term "influence." Therefore, aside from relatively minor terminology differences, we believe the objectives of both approaches are consistent.

[15] Graham Allison and Andrei Kokoshin, "The New Containment: An Alliance Against Nuclear Terrorism," *The National Interest* 69 (2002) 40.

[16] Ashton Carter, John Deutch, and Philip Zelikow, "Catastrophic Terrorism: Tackling the New Danger," *Foreign Affairs* 77.6 (1998) 86.

[17] Barry R. Posen, "The Struggle against Terrorism: Grand Strategy, Strategy, and Tactics," *International Security* 26.3 (2001-2002) 44.

[18] Katie Teitel, Aaron Danis, and James Van De Velde, personal interview, 17 Dec. 2002.

[19] For example, the Brentwood mailing facility is still being decontaminated over one year after the anthrax mailings.

[20] Radio Australia. *APEC: Economic Consequences of Terrorism*, 27 Feb. 2003. <http://www.abc.net.au/ra/asiapac/programs/s793689.htm>.

[21] Paul D. Davis and Brian Michael Jenkins, *Deterrence & Influence in Counterterrorism* (Santa Monica, Calif: RAND, 2002) 67.

CHAPTER 3: A FRAMEWORK TO EVALUATE DETERRENCE-BASED APPROACHES

INTRODUCTION

During the Cold War, the U.S. relied primarily on deterrence to prevent nuclear attacks on the U.S. homeland. Defenses were costly and technologically infeasible, and outright defeat of the Soviet Union was implausible due to the vast arrays of nuclear weapons deployed by both sides. According to Dr. Keith Payne:

> The underlying assumption was that neither side, being rational and reasonable, would intentionally initiate a war if the end result could be widespread mutual destruction. In the context of mutual vulnerability, confidence in deterrence became a tautology: Any rational leader would be deterred from severe provocation by the fear of mutual nuclear destruction; national leaders are rational (how else could they climb to positions of responsibility?); thus, nuclear weapons would deter.[1]

Some experts have dismissed deterring terrorist organizations because they feel terrorists are neither rational nor reasonable by Western standards. Others, like Robert Jervis of Columbia University, think the rationality assumption gives us a false sense of security, and it is more important to understand the group's decision-making processes and perceptions. He writes:

> None of this is to deny the fruitfulness of theories of deterrence that assume rationality and try to deduce state behavior from the external environment. We could not begin … without the baseline of expectations generated by these theories. But they will rarely suffice for a full understanding and, in many areas, are misleading. Melding them with a study of how statesmen perceive others, process incoming information, and reach decisions can give us a richer and more accurate understanding of deterrence.[2]

The Jervis interpretation forms the basis of our approach. Our intent is to derive enough information about the terrorist group to assess future actions and identify potential vulnerabilities without making an assumption of rationality. Patrick Morgan described this as developing a "typology" of the actor.[3] In our opinion, this typology, and the vulnerabilities derived from the detailed knowledge of the organization, can form the basis of deterrent strategies. Our key assumptions are as follows:

- The terrorist organization may or may not be rational by Western standards.

- As defined in Chapter 2, deterrence consists of threats of reprisal, denying an adversary from obtaining his objectives, and the limited use of rewards to undermine the terrorist organization's support base. The objective is to modify the terrorist organization's behavior.

- There are terrorist organizations that by today's standards have both the intent and potential capability to acquire or develop WMD.

- The U.S. will continue to proceed with Defend and Defeat strategies outlined in its "National Strategy to Fight Weapons of Mass Destruction."

- Deterring a critical element or node within the terrorist system may be sufficient to deter a WMD attack.

OVERVIEW OF THE MODEL

The challenge of understanding a terrorist organization's ideology, operational capabilities, motivations, and sources of support is daunting. Without an intellectually rigorous approach, vital strategy elements may be overlooked. What seems to be lacking in the literature on this question is an approach to determining what level of effort should be devoted to deterring terrorists from employing WMD. We believe our model fills that void.

During our interview with William H. McRaven, National Security Council (NSC) Director of Strategy and Defense Issues, Office of Combating Terrorism, he suggested "anything to allow policymakers to visualize steps is a good thing."[4] The SASM model depicted in Figure 2 on the next page complies with his sentiments and illustrates our four-step process to address the question of whether or not it is possible to deter terrorists from using WMD on the U.S. homeland.
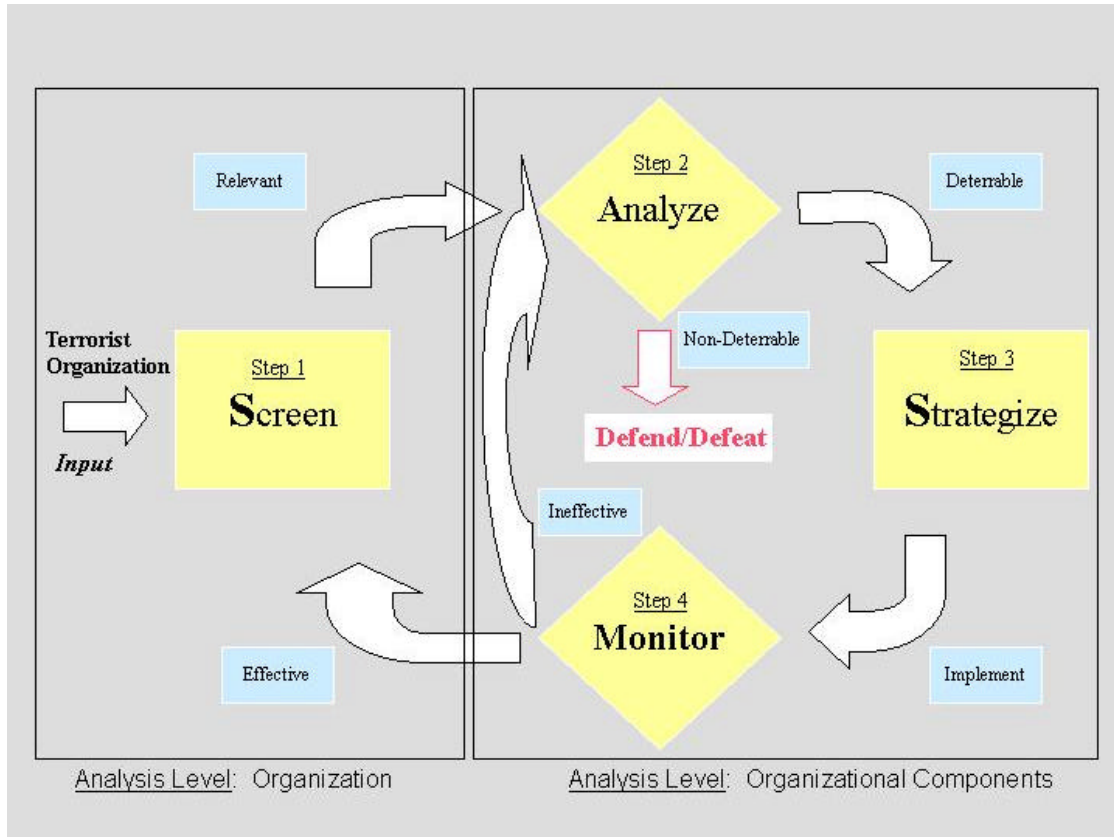
Figure 2: SASM Model

The basic steps of the model involve: **STEP 1 – SCREEN** to determine if the organization has either the capability or intent to employ WMD; **STEP 2 – ANALYZE** organizational goals and decision-making processes; **STEP 3 – STRATEGIZE** deterrence-based approaches if Step 2 suggests there are organizational vulnerabilities; and **STEP 4 – MONITOR** to determine if the organization is responding positively to any of the Step 3 strategies. If the strategies appear effective we re-screen and, if appropriate, exit the model. If the strategies appear to have no effect, then we re-enter at Step 2 and search for an alternative approach.

One difficulty associated with terrorist organizations having the capability to employ WMD is that they contain many components. In their monograph on "Deterrence & Influence in Counterterrorism," Paul Davis and Brian Jenkins of the RAND Corporation use al Qaeda to make their point:

14

It is also important to recognize that al Qaeda does not have a single "center of gravity" whose destruction would bring down the whole organization. Nor does the United States have the information that would enable it to pursue such a finely tuned strategy. Consequently, the United States should adopt a broad-front strategy aimed at influencing the many different parts of the al Qaeda system.[5]

John Parachini and Kim Cragin, also of RAND Corporation, view terrorist organizations as a "networked system as opposed to a homogeneous entity."[6] Davis and Jenkins further emphasize that "[e]ven if the terrorists are not generally deterrable, specific terrorist actions may be deterrable …" and that these certain actions, once deterred, could serve to achieve deterrence of the overall organization for at least some period of time.[7] Our research is consistent with the finding that certain elements of an organization may be deterrable, while others may not. Different deterrent-based strategies might be useful against one component, while other components of the organization may require an entirely different approach.

To account for the complexity of potential adversaries, we believe Steps 2-4 of our model should be run separately for different levels within the target organization. Figure 3 graphically illustrates our approach. At the **STRATEGIC LEVEL**, we include top-level leadership, ideologues who provide the underpinning for the organization's grievances or political motivations, and state sponsors who provide technological support or safe haven. At the **OPERATIONAL LEVEL**, we identify facilitators who form the logistical, financial, and scientific support required to conduct a WMD attack. At this level, we include regional coordinators, scientists, logisticians, training elements, recruiters, intelligence assets, financiers, and any other cells organizing and facilitating operations. Finally, at the **TACTICAL LEVEL**, we consider cell leaders, on-scene reconnaissance and surveillance assets, and the foot soldiers who carry out missions.[8]

By employing this three-tiered approach, we feel the policymaker can uniquely target different levels of the organization and develop more finely tuned deterrent-based strategies. In fact, if you can deter one key component of the organization from providing support, you might successfully prevent a WMD attack, at least for a period of time.

15
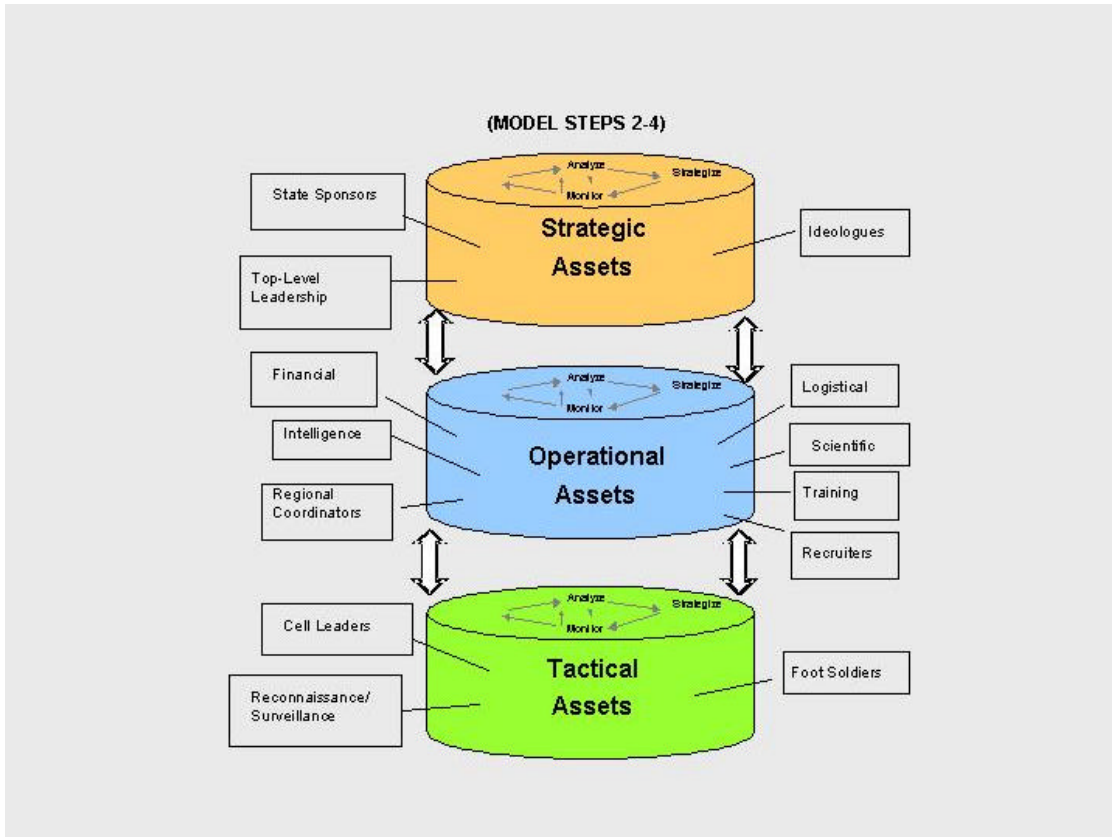
(MODEL STEPS 2-4)

Figure 3: Organizational Level Analysis

DETAILED DESCRIPTION OF THE SASM MODEL

Step 1: Screening – Is the Organization of Interest?

Not all terrorist organizations have a desire to procure or employ WMD. Considering the potential for catastrophic damage and loss of life, WMD employment might not facilitate the achievement of every terrorist group's goals and objectives. In fact, in most cases, it will be detrimental to their cause by eroding popular support. The first step of our approach is to screen out those organizations having no inclination to pursue WMD terrorism and highlight those that do. Our model employs two basic tests to determine the groups deserving further attention: intent and capability.

Intent. In his article on the 1982 British-Argentinean Falklands War, Richard Ned Lebow of The Ohio State University faults the British Intelligence Community for not picking up on Argentina's pre-war signals. He writes:

> However, the problem of repetitive threat neither excuses nor fully accounts for the poor judgment of the British government. Faced with the prospect of recurring crises, it was incumbent upon the British to develop indicators to help distinguish bluff from the real thing. This they failed to do. Instead, London waited for indisputable evidence of impending attack.[9]

Given the cataclysmic consequences of being wrong in discerning the intent of a terrorist organization, we have set the bar low to include all organizations that may have written or proclaimed a desire to acquire or use WMD. Key questions that must be asked are summarized in Table 1. Any organization deemed to have untoward intent is passed on to the next step of our model.

Capability. Capability is an even more telling signal that should highlight the need for further analysis. McRaven of the NSC views technical capability as a more important factor than intent. In his view, intent can change on short notice. Organizations having the prerequisite technical, financial, logistical, and operational capabilities are of immediate concern to the NSC.[10]   Key questions addressing an organization's capability to employ WMD are also summarized in Table 1.

TABLE 1: STEP 1 SCREENING QUESTIONS

Intent
a. Could the organization perceive a benefit or achieve a known goal by employing WMD on the U.S. homeland?
b. Has the organization stated a desire to acquire or employ WMD?
Capability
a. Does the organization have the technical capacity to employ WMD?
b. Is there evidence of effort to acquire WMD capability?

Step 1 Summary

Due to the horrific consequences of being wrong about a group's capability or intent, we intentionally set the screening bar low for the purposes of our evaluation. If the answer to any one of the questions listed in Table 1 is affirmative, the organization is passed to Step 2 of the model for further analysis.

Step 2: Analyze – Is this Level of the Organization Deterrable?

Step 2 is the heart of the SASM model. First, we developed a typology of organizational components to determine motivations, decision-making networks, financial assets, and capabilities. Second, while development of the typology is essential, it is also important to project how the potential adversary views U.S. capabilities. Jervis explains this approach in his book, Psychology and Deterrence:

> Many questions are best addressed by focusing on both sides. Fruitful here is the framework of a mediated stimulus-response model in which one first looks at one state's behavior and the impact it expects its actions to have on its adversary and then examines how the policy is perceived by the other side, how it responds, and how it expects its response to be interpreted. Attention is then shifted back to the first state to see how the response is interpreted and how the cycle continues.[11]

The SASM model incorporates aspects of this approach by including several key questions focusing on how the terrorist organization's components view U.S. capability and will. In addition, Step 2 includes an analysis of the ability of the sides to communicate with each other, another key aspect of deterrence.

At the conclusion of Step 2, the policymaker has enough information to make a Deter, Defend, or Defeat allocation decision for each level of the organization. As depicted in Figure 3, analysis is conducted at the strategic, operational, and tactical levels.

U.S. Analysis of the Organizational Component

Dr. Keith Payne highlights the need for fully exploring the goals, motivations, decision-making processes, and capabilities of so-called rogue states in his book entitled The Fallacies of Cold War Deterrence and a New Direction. His words are equally applicable to non-state actors pursuing the use of WMD:

> There is no adequate alternative to the hard task of attempting to ascertain the particular opponent's modes of thought and core beliefs, assessing how they are likely to affect its behavior, and formulating U.S. deterrence policy in light of those findings. In the absence of this, expectations about the behavior of that particular leadership will reflect a dangerous ignorance.[12]

The SASM model takes on this hard task by evaluating components at each of the three levels on the basis of five key areas: goals and ideology; network structure; financial structure; technical

capacity; and operations capacity. In each area, the model explores key elements of organizational power or structure to develop a clear picture of the organization's assets and vulnerabilities.

1) Goals and Ideology

Jervis underscores the need to understand the values and beliefs of the adversary when making policy decisions: "A first step is to grasp the other side's values, beliefs, and perceptions and to understand the motivated and unmotivated biases that influence information processing and decision making."[13] Jerrold Post of George Washington University cites historical, cultural, and contextual features as key indicators of increasing levels of terrorist violence.[14] Underpinned by these sources, the SASM model asks four key questions to discern the goals and ideology of the organization. They are summarized in Table 2.

TABLE 2: U.S. ANALYSIS OF ORGANIZATION (GOALS & IDEOLOGY)

a.   What are the vision and purpose of the component?
b.   Is the component religiously motivated?
c.   Is self-preservation of the component essential to itself or the larger organization?
d.   How committed to the cause is this component of the organization?

2) Network Structure

Network structure is another key area that must be understood. To have any chance of deterring elements within a terrorist organization, one must understand how these components interact, how leaders exercise command and control, and whether or not elements within the organization might be targetable. Steven Simon and Daniel Benjamin, for example, describe al Qaeda's command and control structure as a combination "hub and spoke" structure (where nodes communicate with the center) and "wheel" structure (where nodes in the network communicate with each other without reference to the center). "This is a structure that combines resilience with command and control, complicating efforts to root out cells and disrupt operations."[15]

Key questions concerning the network structure are presented in Table 3.

TABLE 3: U.S. ANALYSIS OF THE ORGANIZATION (NETWORK STRUCTURE)

a. Does the component have a coherent command and control structure, and how does it receive direction from higher levels of the leadership chain?
b. How much of the command and control structure is horizontally distributed?
c. How does it communicate with lower levels of the leadership chain?
d. Do targetable elements exist?
e. Do we know who the leaders of the component are and where they are based?
f. Do these leaders have the authority and control to launch or abandon operations by subordinate cells?
g. How dispersed geographically is this component of the organization?

3) Financial Structure

Financial structure is another key area that may be a likely target for deterrent-based strategies. According to Davis and Jenkins, "Bin Laden may feel he has nothing to lose, but at least some of his financiers live comfortably with wealth, family, and prestige. Obviously, they do have something to lose."[16] The SASM model questions addressing finances are included in Table 4.

TABLE 4: U.S. ANALYSIS OF THE ORGANIZATION (FINANCIAL STRUCTURE)

a. What are the sources of the component's income?
b. Does the component generate/contribute sufficient funds to develop WMD?
c. Does the component generate/contribute sufficient funds to purchase WMD?

4) Technical Capacity

Technical capacity is essential if a terrorist organization is to pursue a WMD strategy. Given the difficulty associated with procuring, developing, deploying, and employing these weapons, understanding the group's technical capabilities is essential. RAND terrorism expert Bruce Hoffman explains that these capabilities are not limited to nuclear, chemical, and biological weapons components. "For bin Laden, the weapons of modern terrorism critically are not only the traditional guns and bombs, but also the mini-cam, videotape, television and Internet."[17] Simon and Benjamin also warn that WMD components need not always come from a state sponsor:

Acquiring WMD or materials need not depend on the collaboration of a state sponsor. Terrorists appear increasingly eager to purchase weapons or components, possibly from pilfered stocks of the former Soviet Union or from the broad array of dual-use materials and equipment found on the open market.[18]

Model questions delving into the technical capacity of the organization are listed in Table 5.

TABLE 5: U.S. ANALYSIS OF THE ORGANIZATION (TECHNICAL CAPACITY)

a. Does the component have a scientific infrastructure capable of independently weaponizing WMD?
b. Is the component dependent on external technical expertise?
c. Has the component received WMD materials/items from another state?
d. Has the component received WMD materials/items from a non-state entity?
e. Are we aware of any WMD testing?

5) Operations Capacity

The system's capability to conduct operations must be understood to fully address the question of deterrence. Hoffman writes that conducting coordinated operations, for example, is very difficult.

For reasons not well understood, terrorists typically have not undertaken coordinated operations. This was doubtless less of a choice than a reflection of the logistical and other organizational hurdles and constraints that all but the most sophisticated terrorist groups are unable to overcome.[19]

Davis and Jenkins further amplify this sentiment when they write, "To the contrary, the empirical record shows that even hardened terrorists dislike operational risks and may be deterred by uncertainty and risk."[20] Key vulnerabilities might be uncovered by a thorough understanding of a potential adversary's capacity to execute operations. SASM Model questions for this area are summarized in Table 6 on the next page.

TABLE 6: U.S. ANALYSIS OF THE ORGANIZATION (OPERATIONS CAPACITY)

a. Does this component of the organization have a record of novel attack methods?
b. Is there an increasing pattern of lethality or indifference to the scale of casualties involved in past actions?
c. Does the component have a history of committing suicide attacks?
d. Has the component conducted, coordinated, and synchronized operations with other organizational components?
e. Does the component have an effective means of conducting information operations?
f. Are there essential and identifiable training facilities tied to this level of the organization?

Organization's Perception of U.S. Capability and Will

Deterrence is a psychological concept, and to a large degree, success or failure is dependent upon your adversary's view of your capability and will. With WMD, the stakes are very high. Robert Jervis notes "The credibility of one threat is linked to that of others, and states therefore must be willing to pay high costs for minor stakes if they are to deter others from challenging their vital interest."[21] The SASM model ensures that four factors are considered through the eyes of a terrorist adversary bent on employing WMD: past U.S. behavior; U.S. intelligence capabilities; U.S. Defend capabilities; and U.S. Defeat capabilities.

1) Past Behavior

Table 7 highlights what may have been al Qaeda's view of U.S. capability and will prior to its 9/11 attacks.[22] The story told by Table 7 on page 24 portrays weak U.S. resolve as seen from al Qaeda's perspective. This is despite the possibility that U.S. actions in Afghanistan and elsewhere may eventually act to modify its opinion of U.S. determination to prevent future catastrophic events.

TABLE 7: RESPONSE TO ISLAMIST TERRORIST ATTACKS PRIOR TO SEPT 11

Year	Attack	Overt U.S. Military Response
1983	Beirut	Withdrawal
1984-86	American Hostages in Lebanon	U.S. concessions to buy freedom of hostages
1993	Mogadishu	Withdrawal
1998	Al-Khobar Towers	None
1998	Kenya/Tanzania	Cruise-missile attacks
2000	USS Cole	None

Key questions for evaluating U.S. capability and will from the terrorist organization's perspective are listed in Table 8.

TABLE 8: PERCEPTION OF U.S. CAPABILITY AND WILL (PAST BEHAVIOR)

a. Have the U.S. or its allies directed action against this component of the organization in the past? Was it effective?
b. Has the U.S. acted against states supporting the target organizational level? Was it effective?
c. Has the U.S. successfully acted against other states or terrorist groups in a way that could serve as a "lesson?"
d. Has the U.S. successfully led an international coalition in response to terrorist threats?
e. Has the U.S. articulated a clear doctrine regarding WMD use on the U.S. homeland since the end of the Cold War? Has this message been consistently translated by all levels and branches of government?
f. Has the U.S. conducted information operations/public diplomacy convincing to the terrorist organization's bases of support?

2) Intelligence Capabilities

One cannot underestimate the impact that effective, timely, and accurate intelligence can have on this effort. Kurt Campbell and Michèle Flournoy suggest intelligence will be pivotal in the war on terror, stating, "Intelligence is crucial in any war, but it comes close to the defining factor in this campaign."[23] Essential questions looking at U.S. intelligence capabilities from the potential adversary's perspective are outlined in Table 9 on the next page.

TABLE 9: PERCEPTION OF U.S. CAPABILITY AND WILL (INTELLIGENCE CAPABILITIES)

a. Does the organizational component believe the U.S. Intelligence Community has the capability to anticipate its operations?
b. Has the U.S. disrupted previous activities on the basis of accurate and timely intelligence?
c. Has the U.S. effectively coordinated intelligence operations and shared intelligence information with other countries?
d. Has the organizational component modified its modus operandi as a result of U.S. intelligence activities?

3) Defend Capabilities

Davis and Jenkins make a strong case that defensive preparations can have a deterrent effect. "Aside from their direct value for defense per se, such preparations and their exercise could contribute significantly to deterrence by helping to dispel the notion that the United States can be easily toppled."[24] In fact, they feel strongly that considerable U.S. efforts at building defenses should be to "communicate a sense of that American capacity to adapt and recover."[25] Important defend questions are listed in Table 10.

TABLE 10: PERCEPTION OF U.S. CAPABILITY AND WILL (DEFEND CAPABILITIES)

a. To what degree have U.S. defensive measures dissuaded terrorists from pursuing WMD attacks against the U.S. homeland?
b. To what degree has the international community dissuaded terrorists from pursuing a WMD strategy?
c. What is the cost to the organization should a WMD attack on the U.S. homeland be foiled, in terms of: prestige? initiative? support?

4) Defeat Capabilities

While this paper focuses on deterrence, certain Defeat strategies can also have a deterrent effect. Davis and Jenkins write about the effect near-term actions can have on longer-range goals:

The tactic of crushing terrorists to deter future actions deserves elaboration. Some of the current actions to destroy al Qaeda will contribute to general deterrence later, especially if the United States is seen as strong and relentless.[26]

We recognize that we cannot go too far with crediting Defeat measures as deterrence. One could basically cite everything under the deterrent banner, thereby making the word defeat meaningless. For the purposes of this paper, we will limit our discussion of Defeat capabilities to those near-term and limited objectives aimed at eliminating minor organizational elements with an objective of deterrence as opposed to outright eradication of the organizational component. The idea would be to get inside the minds of the terrorist operatives to instill fear among the others, not outright elimination of the entire network. Key self-examination questions concerning U.S. Defeat capabilities are listed in Table 11.

TABLE 11: PERCEPTION OF U.S. CAPABILITY AND WILL (DEFEAT CAPABILITIES)

a. Are there credible threats the U.S. can communicate?
b. Does the U.S. have the political will to use them?
c. What are the costs to delivering on the threat?
d. What are the costs associated with taking no action?

Ability of the Sides to Communicate

Given that deterrence is based on perceptions, one cannot underestimate the importance of communications channels. Lebow underscores this aspect when he writes:

The success of deterrence as a strategy of conflict avoidance depends not only upon the capability and resolve of the defender of a commitment but just as much upon its ability to communicate that capability and resolve to adversaries.[27]

The SASM model focuses on two key aspects: U.S. capability and willingness to communicate with the potential terrorist organization, and the terrorist organization component's ability to receive U.S. signals.

1) U.S. Capability to Communicate with the Organizational Component

The U.S. government is reluctant to communicate directly with terrorist organizations. First, it is often unclear which component within the system to communicate with. Secondly, the U.S.

government should not be viewed as openly negotiating with terrorists lest such negotiations encourage further terrorism. Sending signals covertly or through third parties has associated risks, too. Lastly, general communication over public media or through official government pronouncements or policies has the potential to be misunderstood or dismissed. All of these issues are vetted in the SASM model's Step 2 Communications analysis. Specific questions are listed in Table 12.

2) Component's Ability to Receive Signals

The terrorist organization component's ability to receive U.S. signals is equally important. Lebow highlights cultural and linguistic issues associated with message receipt:

> Deterrence theorists tend to ignore difficulties that might be associated with the actual signaling process. They generally assume that adversaries, who usually speak different languages, nevertheless share common symbols that facilitate effective communication.[28]

The problem with terrorist organizations is precisely that they do not "share common symbols that facilitate effective communications." Thus, this category assumes great importance, as does understanding the psychological make-up of the group. Questions associated with message receipt are also listed in Table 12.

TABLE 12: ABILITY OF THE SIDES TO COMMUNICATE

U.S. Capability to Communicate with the Organizational Component
a. Can the U.S. Government communicate unambiguously with this component of the organization?
b. Can the U.S. Government communicate with a state or non-state actor who has the ability to communicate with the target component?
Component's Ability to Receive Signals from the U.S.
a. Can the component receive and comprehend intended messages from the U.S. Government?
b. Does the component have the ability to communicate unambiguously with the U.S. Government?

Step 2 Summary

Armed with the answers to the Step 2 questions, it is now incumbent on the policymaker to determine a Deter, Defend, or Defeat strategy mix. If the Step 2 analysis identifies components with vulnerabilities to deterrence-based strategies, those components move forward to Step 3 strategy options. If, on the other hand, components such as top-level leadership are so hardened, uncommunicative, and bent on cataclysmic outcomes as to suggest that no deterrent strategy will be

effective, then they get slated for Defend or Defeat attention. With the detailed analysis outlined in Step 2, the policymaker will have a better basis upon which to make this all-important strategy allocation decision.

Step 3: Strategize – Option Development and Implementation

Strategy development will be driven by the vulnerabilities and other outcomes of Step 2 analysis. It is essential to allow the analysis to drive the policy rather than the reverse. Making untoward and unpromising threats that cannot be carried out and have little chance for success can be counterproductive. One has to be willing to fulfill promises to obtain the benefits of one's pronouncements. Payne expounds on this point in his treatise on the fallacies of Cold War deterrence:

> The optimal U.S. deterrence policy ideally would be informed by these factors. That is, the U.S. force structure, threat, and declaratory policy, for deterrence purposes, are the dependent variables; they are not the starting points of consideration. To a large extent they should be derived from findings about the challenger and the context. This seemingly logical sequence, unfortunately, is not the norm.[29]

Davis and Jenkins advocate what they term a "broad front strategy." They espouse the following as the key attributes of a counterterrorism strategy.

- Manifest strength and, perhaps even more important, manifest purpose and determination
- Relentlessness and effectiveness of actions
- Consistency with American values and moral validity apparent to others
- A balanced mid- and long-term strategy that includes both coercive measures and inducements[30]

It is impractical to predict the types of deterrence-based strategies that might be successful when confronting organizations pursuing WMD employment. There is no single toolbox from which to select policies and strategies. The SASM model does, however, direct the policymaker to consider specific elements of U.S. power and apply them to the vulnerabilities identified in Step 2. The user of the model applies this step to determine exploitable vulnerabilities. A summary of Step 3 questions requiring high-level attention is outlined in Table 13 on the next page. Again, this analysis is conducted separately for each of the three levels that were outlined in Figure 3 on page 17.

TABLE 13: STEP 3 STRATEGIZE

1. What are the key vulnerabilities of this component of the target organization?
2. What vulnerabilities can the U.S. successfully target?
a. Military (e.g., operations, train host nation counter-terrorist forces)
b. Economic (e.g., freezing assets, funding counter-terror campaigns)
c. Political/Diplomatic (e.g., counter-terror coalition building)
d. Legal (e.g., bringing terrorists to justice, strengthening laws)
e. Information Operations (e.g., fracturing organizational cohesion, isolating leadership, inciting mistrust, prying away public support, molding/mobilizing world opinion)
3. Where else can the U.S. derive support for its policies?
a. UN
b. Allies
c. Regional organizations
d. Non-state actors such as non-governmental organizations (NGOs)
e. World opinion
4. What are the organizational component's capabilities to respond?

Step 3 Summary

The outcome of this step will yield a series of policy options that the policymaker can choose to implement. Some component levels of the organization will likely be targeted by deterrent strategies. (Others, however, may not have passed beyond Step 2 of the model and are slated for Defend or Defeat efforts.) Following Step 3 implementation, the components are forwarded to Step 4 for monitoring.

Step 4: Monitor – Evaluate Option Effectiveness

During the 40-plus year Cold War, the U.S. and the Soviet Union had multiple opportunities to assess each other's capabilities and intent. Through face-to-face Strategic Arms Limitation Talks (SALT) and Strategic Arms Reduction Talks (START), American and Soviet experts discussed strategy and the implications of advances in both the quality and quantity of each other's nuclear arsenals. In addition to formal talks, cultural interchanges, economic trade, sessions at the United Nations, and other open meetings provided both sides the opportunity to understand each other's view of the world. The intelligence communities of each side monitored strategic modernization programs, operations tempo, and troop movements. One could often detect new missile silos being built or

bombers and submarines being flushed in the air or at sea. While there was always the chance of miscalculation or a bolt-out-of-the-blue attack based on deception and a covert plan, the U.S. coexisted with the Soviet Union in a relatively stable and transparent environment.

This is in stark contrast to the environment we now share with terrorist organizations that may be interested in using WMD on the U.S. homeland. The U.S. does not have formal or even informal relationships with these organizations and does not have the benefit of several decades of interchange and communication. It is much more difficult for the Intelligence Community to gather information about both capability and intent. There are no missile silos to count, and operations tempo is difficult to discern.

Information Sources. Nearly every attempt to gauge both interest and progress on a terrorist group's efforts to use WMD will rest on inside information and the U.S. Intelligence Community's ability to derive knowledge from primary sources. Developing a robust human intelligence capability will be essential to monitoring non-state actors' future plans. While getting inside top-level leadership may not be possible, it is essential to develop sources as close to the inner circle of terrorist decision-makers as possible. A more achievable goal might be to target those groups or individuals providing operational level support as described in Figure 3. Logisticians, financiers, scientists, trainers, and recruiters can all provide valuable information when determining whether or not a deterrent strategy is having the desired effect. Electronic information-gathering capabilities are beyond the classification level of this paper but may also be used to determine network noise levels and communications channels. Clearly, many terrorist groups have taken advantage of the Internet to give orders and plan operations. The U.S. National Security Agency may be able to exploit this arena with its vast array of technical capabilities. Finally, the least reliable but potentially most useful information-gathering source is the international voice and print media. While one cannot believe every pronouncement one sees or reads, the media do have an extensive human collection network for information and so may be useful to consult when evaluating overall levels of interest in WMD weapons.

Measures of Effectiveness. When considering potential Step 3 strategies, the policymaker should simultaneously consider how to measure success or failure. While it is difficult to craft generic measures of effectiveness (MOE) that apply to every case, and even more difficult to collect reliable data, policymakers should at least attempt to consider such performance measures as:

- Internal network noise levels
- Interview results of captured operatives

- Movements of scientific and logistical operatives

- Evidence of WMD testing

- Changes in black market WMD component price levels

- Unusual money movements

- Levels of violence associated with non-WMD events if indicative of changes in operations capability

- Complexity and organizational coordination of non-WMD events if indicative of changes in operations capability

- Open source communications addressing WMD

- Sentiment in communities known to support the group

- Numbers of close followers of inflammatory religious leaders

- Grossly inflated and/or deflated prices of specific goods

- Increasing levels of sophistication in terrorist attacks

Active Probing. The U.S. cannot afford a passive approach to Step 4. Strong consideration should be given to actively injecting an input into the terrorist network while measuring the impact the input has on the organization's interest level and response. For example, when trying to measure a target group's interest level in acquiring nuclear material on the black market, U.S. supported operatives might attempt to sell defective quantities of the material or faulty components to judge the organization's interest level. Another approach might be to use insider information derived from interrogations of captured operatives to provide a credible stimulus into the system as a means of provoking a measurable response from it. While these types of operations might not be appropriate in all cases, they are important because passive intelligence-gathering measures alone will not fulfill Step 4 monitoring requirements.

Step 4 Summary

A summary of Step 4 questions is listed in Table 14 on the next page. At the conclusion of this step, the policymaker must determine whether the strategies implemented from Step 3 are having the desired effect. If the Step 4 MOE are moving in a positive direction, the organization might be moved back to Step 1 for re-screening. If the group is unresponsive to Step 3 measures, then it may

be necessary for re-analysis at Step 2, which could lead to a revised Deter-Defend-Defeat strategy allocation.

TABLE 14: STEP 4 MONITOR

1. Have the intent and capability of the organizational component changed sufficiently to merit re-screening?
2. Has the component of the organization responded positively to the deterrent strategy?
3. Are there measures of effectiveness available to determine success or failure?
4. What are the measures of effectiveness that should be continuously evaluated?

CONCLUSION

The four-step SASM model is intended to formalize a disciplined and intellectually robust effort to determine the contribution that deterrence-based strategies can make in dealing with the problems associated with terrorist groups having a desire to use WMD on the U.S. homeland. While the questions listed in each of the four steps above are intended to be detailed and insightful, by no means are they comprehensive or exhaustive. It is expected that as the policymaker attempts to accomplish each of the steps listed above, additional questions will come to mind. The analytic model provided above serves as a starting point for this effort.

---

[1] Keith Payne, *The Fallacies of Cold War Deterrence* (Lexington, Kentucky: The University Press of Kentucky, 2001) 17-18.

[2] Robert Jervis, Richard Ned Lebow, Janice Gross Stein, *Psychology and Deterrence* (Baltimore and London: The Johns Hopkins University Press, 1985) 11.

[3] Jervis, Lebow, and Stein 126.

[4] William H. McRaven, personal interview, 18 Dec. 2002.

[5] Paul D. Davis and Brian Michael Jenkins, *Deterrence & Influence in Counterterrorism* (Santa Monica, Calif: RAND, 2002) xiii.

[6] P. A. Parachini and Kim Cragin, personal interview, 19 Dec. 2002.

[7] Davis and Jenkins 59.

[8] By Strategic we refer to the functions responsible for issuing guidance and defining grand strategy. Operational level refers to those components that plan and coordinate operations or provide non-state logistical, financial or technical support. By tactical level we refer to the individuals who execute operations.

[9] Jervis, Lebow, and Stein 93.

[10] McRaven personal interview.

31

[11] Jervis, Lebow, and Stein 2.

[12] Payne 99.

[13] Jervis, Lebow, and Stein 3.

[14] Jerrold M. Post, Keven G. Ruby, and Eric D. Shaw; "The Radical Group in Context: 1. An Integrated Framework for the Analysis of Group Risk for Terrorism," *Studies in Conflict & Terrorism* 25 (2002) 78.

[15] Steven Simon and Daniel Benjamin, "America and the New Terrorism," *Survival* 42.1 (2000) 70.

[16] Davis and Jenkins 15.

[17] Bruce Hoffman, "Re-Thinking Terrorism in Light of a War on Terrorism," Testimony before the Subcommittee on Terrorism and Homeland Security, House Permanent Select Committee on Intelligence, U.S. House of Representatives (Washington, DC: RAND, 26 Sep. 2001) 10.

[18] Simon and Benjamin 72.

[19] Hoffman, "Re-Thinking Terrorism in Light of a War on Terrorism" 8.

[20] Davis and Jenkins xii.

[21] Jervis, Lebow, and Stein 9.

[22] Davis and Jenkins 27.

[23] Kurt M. Campbell and Michèle A. Flournoy, *To Prevail* (Washington, DC: The CSIS Press, 2001) 25.

[24] Davis and Jenkins 16.

[25] Davis and Jenkins 16.

[26] Davis and Jenkins 10.

[27] Jervis, Lebow, and Stein 205.

[28] Jervis, Lebow, and Stein 205.

[29] Payne 102.

[30] Davis and Jenkins 25.

CHAPTER 4: A CASE STUDY APPLICATION OF THE SASM MODEL - AL QAEDA

Can al Qaeda be deterred? Of course not. But wait, what do we mean by that? If we ask, instead, whether elements of the al Qaeda system can be deterred from doing specific things, the answer is "Yes." [1]

Al-Qaeda is the principal terrorist organization that has attempted to engage in mass destruction attacks on the United States. … Other terrorist organizations, however, must be kept under surveillance and attacked preemptively if they seem ready to strike the United States or its allies in mass attacks, or if they appear intent on aligning themselves with al-Qaeda. [2]

Although they are elements of a Defeat strategy, the arrests in early 2003 of Khalid Shaikh Mohammed, chief of al Qaeda operations, and Sheik Mohammed Ali Hasan al-Moayad, a linchpin in al Qaeda global financing with Muslim charities, certainly serve as a deterrent to others in the system. What this means for a U.S. strategy that recognizes deterrence as viable is that the U.S. should pursue measures that capitalize on the deterrent aspects of such arrests. It should actively engage in operations publicizing to others in the al Qaeda network that they, too, would eventually be apprehended if they continue to support terrorist operations. This may well deter those components that are either wavering in their commitment or who have things they value and do not want to risk losing.

Since its 9/11 attacks on the U.S. in 2001, the al Qaeda terrorist system has come under close scrutiny for the threat that it poses. Bin Laden, the group's leader, has claimed to have chemical and nuclear weapons and to be prepared to use them against the U.S. The wealth of information uncovered in the aftermath of 9/11 indicates that it is likely that al Qaeda has both the intent and the potential capability to employ WMD on the U.S. homeland. As such, it is the most reasonable organization to use as we evaluate both the limits and the utility of the SASM model.

METHODOLOGY

We have used only open source material for this case study. While access to classified data would produce a more reliable analysis, the purpose of this case study is to demonstrate the utility of the model rather than to develop a strategy against al Qaeda. With this in mind, our methodology is to answer each of the questions outlined in Chapter 3 and then draw conclusions from those answers that could be shaped into a deterrence strategy. Concurrently, measures of effectiveness were derived.

Step 1 analysis was conducted on the organization as a whole while the analysis in Steps 2 through 4 was carried out sequentially for the strategic, operational, and tactical levels of the al Qaeda system.

Step 1: Screening – Is the Organization of Interest?

The first step of the SASM model is to screen out the many terrorist organizations that do not currently present a significant threat of using WMD against the U.S. homeland.   As the following quote from bin Laden in November 2001 shows, our analysis suggests al Qaeda is presently the foremost non-state actor who has both the stated intent and the capability to employ WMD on the U.S. homeland: "… we have chemical and nuclear weapons as a deterrent and if America used them against us we reserve the right to use them." [3]

Intent

Al Qaeda has a history of conducting spectacular attacks as a way of boosting its image among its support base as well as demonstrating its capability.   The 9/11 attacks on New York and Washington demonstrate its penchant for such attacks on the U.S. homeland.   Furthermore, referring to nuclear and chemical weapons, bin Laden said in an interview with Hamid Mir: "We have the weapons as a deterrent." [4]   Accordingly, we conclude that there is a high probability that al Qaeda has the intent to use WMD on the U.S. homeland.

Capability

As indicated above, bin Laden has claimed to have chemical and nuclear weapons. Furthermore, a precursor to the deadly VX nerve agent was found at al Qaeda's facilities near Khartoum in 1998,[5] and plans for al Qaeda to use the poison ricin were found in Kabul in November 2001.[6]   Al Qaeda is also known to have conducted tests of chemical artillery shells to carry an anti-riot paralyzing agent in Sudan, and documentation exists suggesting the organization attempted to purchase uranium from South Africa in 1994 for $1.5 million.[7]

Step 1 Summary

Given the stated intent to use WMD against the U.S., and evidence of WMD testing and claims by al Qaeda that it already has WMD, al Qaeda passes the screening test for further consideration by the SASM deterrence model.

Step 2: Analyze – Is this Level of the Organization Deterrable?

Having screened the organization, we will now analyze the strategic, operational and tactical levels of the al Qaeda terrorist system to identify traits that may be used to deter a WMD attack.

U.S. Analysis of the Organizational Component

1) Goals and Ideology

Strategic Level. Initially, al Qaeda's purpose was to "channel the energies of the Mujahidin into fighting on behalf of oppressed Muslims worldwide, as an Islamic 'rapid reaction force.'" [8] The assassination of Azzam in 1989 allowed bin Laden to assume full control of the organization and to use terrorism in pursuit of his goals of defeating America and Israel.[9] Bin Laden sees these objectives as prerequisites for defeating what he regards as corrupt regimes in the Middle East.

Concerning al Qaeda's ideological motivation, on a tape broadcast by al Jazeera, an Arab satellite channel in the Middle East, bin Laden has stated: "This is a matter of religion and creed; it is not what [President] Bush and [Prime Minister] Blair maintain, that it is a war against terrorism … There is no way to forget the hostility between us and the infidels. It is ideological, so Muslims have to ally themselves with Muslims." [10] Furthermore, Gunaratna has observed that "As long as Osama is Emir General and al-Zawahiri is the principal strategist, [al Qaeda] will not compromise. Post Osama, its psyche will commit its members to his dream and al-Zawahiri's strategy – until or unless Osama's legacy fades away." [11] Bin Laden's tenacious commitment to al Qaeda's goals was well described when Hoffman observed, "for bin Laden, not losing is winning." [12]

States providing safe haven or technical support to al Qaeda must also be considered when conducting analysis at the strategic level. As states have return addresses, they can be targeted and thereby are susceptible to deterrence-based strategies. For example, the Taliban regime in Afghanistan actively supported al Qaeda. Following the 9/11 attacks on the U.S., the Taliban was directly attacked and forced from power. This precedent provides a powerful example of what can happen to rogue states providing WMD support to al Qaeda. Without such state support, al Qaeda would have considerable difficulty developing and testing nuclear weapons in particular. The U.S. administration believes that Iraq poses a similar threat. Accordingly, it has been actively voicing deterrent threats aimed at preventing transfer of WMD from Iraq to al Qaeda. The outcome of this policy approach is not yet known. Pakistan's recent shift of support away from al Qaeda to the WOT indicates the effectiveness of deterrence at the state level.

The senior leadership of al Qaeda appears overly committed to the cause to be effectively deterred, except to the minor extent that successful defeat and defend operations contribute to deterrence by objective denial.   As the deterrent strategy of objective denial on these leaders may not be effective, the U.S. must rely principally on Defeat and Defend strategies with regard to the senior leadership and ideologues associated with al Qaeda. In the case of state sponsors, however, their fixed interests appear to make them deterrable. Accordingly, the U.S. administration must clearly articulate a policy of intervention against all states providing al Qaeda with any level of WMD support. No distinction should be made between the terrorist group conducting a WMD attack and the state providing it with safe haven or technical support.

Operational Level. While the core elements of the operational level of the al Qaeda system are as committed and ideologically motivated as senior leadership, the scale and diversity at this level exposes it to the potential for exploiting internal differences. For example, we have defined the operational level as including not just the al Qaeda operatives, but also wealthy Arab benefactors, WMD scientists, government organizations such as Pakistan's Inter-Service Intelligence (ISI), and Islamic charities like Benevolence International Foundation that have been infiltrated by or collaborated with al Qaeda.   In a network of supporters this diverse and large, it is reasonable to expect varying degrees of commitment to goals that can be targeted by a deterrence campaign, especially given al Qaeda's reliance on a distorted version of Islam.   Those elements have families, businesses, or other identifiable interests that appear targetable, and they are therefore potentially susceptible to deterrence.   Accordingly, it is conceivable that elements will exist at this level that are more concerned with self-interest than ideology.

Tactical Level. The repeated use of suicide operatives, such as the 9/11 hijackers and those involved in the attack on the USS Cole, demonstrates the high level of commitment and ideological motivation of the tactical components as well as their disregard for their own preservation.   Efforts to deter tactical components will succeed only if al Qaeda's ideology and methods can be discredited by credible Islamic figures, thereby eroding the ideological justification and rewards for the foot soldiers committing suicide.   Additionally, addressing the root causes of terrorism, such as Middle East perceptions of uneven treatment of the parties to the Israel-Palestine dispute, may help stem the tide of recruitment. Employment and political empowerment can also help reduce the influence al Qaeda recruiters have when seeking prospective foot soldiers.

2) Network Structure

Strategic Level. The principal authority figures of al Qaeda are bin Laden and Zawahiri.[13] Bin Laden is the Emir General, and he controls al Qaeda through four divisions that are responsible for military operations, finances, fatwa and Islamic study, and media and publicity. A consultative council (Shura Majilis) is used to provide ideological authority to bin Laden's pronouncements, goals, and methods. Functionally, we can regard al Qaeda as comprised of four principal elements: a command and control pyramid, a global terrorist network, a base force of guerillas (based on the 055 Brigade), and, a loose coalition of terrorist and guerilla groups.[14] Since the destruction of the Afghanistan bases, the current locations of the senior leadership are unknown.

Concerning control of subordinate elements, documents relating to planned attacks in Singapore were found in Afghanistan, suggesting that tactical plans are reviewed at the strategic level.[15] This has been further confirmed in statements by captured terrorists asserting that Bin Laden personally indicated where to park the explosives truck in the 1998 East African embassy attack.[16] Because al Qaeda communicates vertically to control attacks, it becomes operationally exposed to disruption. However, because al Qaeda uses highly redundant systems, it is unlikely that deterrence-based approaches can completely sever communications with lower levels of the organization.

Operational Level. As of mid-2001, al Qaeda had a permanent or semi-permanent presence in 76 countries.[17] "The regional node in Bosnia … coordinated operations in the Balkans, its counterpart in Georgia handles the Caucasus, African operations are run from Yemen and Somalia, and Malaysia and Indonesia look after Asia." [18] This structure indicates the capacity to exercise centralized control while retaining regional command and control capabilities, and it allows the organization to operate independently when needed.[19] Communications between higher and lower level components rely principally on trusted person-to-person contact and encrypted Internet traffic.

Since the 9/11 attacks, international efforts have disrupted visible elements at the operational level. However, subsequent simultaneous and coordinated attacks such as those in Bali and Kenya suggest that a high residual capability exists. Affiliated terrorist organizations that may be cooperating with al Qaeda include Jemaah Islamiyah (JI) and Moro Islamic Liberation Front (MILF), considering that their methods and goals are so similar to al Qaeda's as to preclude any clear definition of a boundary between them. Accordingly, the apparent size and diversity of the network structure at this level suggests that deterrence is unlikely to be effective when directed against its communications network.

Tactical Level. As mentioned above, al Qaeda had a presence in 76 countries as of mid-2001, and we know that each cell operates strictly independently of the other[20] to preserve capability should one cell be compromised. Each cell also has a trained leader and is capable of operating independently of the centralized command chain, if required.[21] However, we also know that tactical plans are reviewed at the strategic level, suggesting a bias for centralized control for the major attacks. The diversity of the network at this level means that it is highly unlikely to be effectively deterred.

In summary, al Qaeda can be seen as a complex system involving an ideological core that both conducts its own terrorist attacks and sponsors attacks by ideologically sympathetic organizations. While Simon and Benjamin's hub and spoke model comes close to describing the al Qaeda threat, it does not emphasize the potential autonomy and capabilities of related entities such as JI and the MILF. Another model used to describe al Qaeda is the image of an oak tree dropping metaphorical acorns from which more terrorist entities grow.[22] However, the acorn model fails to depict the degree to which the offspring remain connected to the parent. For our purposes, we have come to think of al Qaeda like a strawberry plant that sends out runners forming roots where they touch the ground to spawn new plants. These new plants remain connected to the parent; however, they can also operate independently if the connection becomes severed. Deterring a network structure of this nature cannot be accomplished as a whole. Ultimately, all traces of the organism must be removed, i.e., defeated. In the interim, strategies aimed at deterring key offspring can reduce the risk of the system obtaining and using a WMD capability. This organic analogy may be helpful in visualizing the distributed and resilient nature of the al Qaeda system.

3) Financial Structure

Strategic Level. Bin Laden is believed to have inherited between $25 and $30 million, which he has invested very broadly and successfully.[23] For example, while in Sudan he established approximately 30 companies ranging in scope from genetic research to civil construction, and he bought two large farms.[24] Bin Laden also invested $50 million in a bank closely linked to the Sudanese elite[25] and $100 million in the Taliban government.[26] To varying degrees Iran,[27] Afghanistan[28] and Pakistan[29] are believed to have supported al Qaeda activities. However, recently the regime in Afghanistan has been forcibly removed, and the regime in Pakistan has formally come to support the war on terrorism. The current position of the Iranian regime with regard to supporting al Qaeda is unknown, although we do know Iran maintains significant influence in western Afghanistan.[30] Al Qaeda also receives funds from infiltrated Islamic charities that collect money in Western countries.

With an estimated annual operating budget of between $36 and $50 million, al Qaeda clearly has considerable financial scope for conducting WMD research.[31] As mentioned in Chapter 2, expert evidence[32] suggests that only a handful of scientists would be required to develop a nuclear bomb, and we also know that al Qaeda attempted to purchase uranium from South Africa in 1994 for $1.5 million. Further, we know that al Qaeda has been conducting research into the toxin ricin and VX nerve gas as well as having tested chemical delivery artillery shells while in Sudan.[33] Accordingly, it seems reasonable to conclude that al Qaeda has had the financial resources to buy and/or develop all three classes of WMD.

The diversity of sources of income, plus the ongoing coordinated terrorist attacks in different regions, suggest that al Qaeda may have retained a significant financial capacity despite the post 9/11 international clampdown on its resources. Accordingly, efforts to deter strategic sponsors, namely states, from providing al Qaeda with financial support must continue. There must be no distinction made between a state that provides financial support and an al Qaeda cell that carries out a WMD attack.

Operational Level. Sources of income at the operational level are known to include a core income of donations made by wealthy Arab benefactors in the United Arab Emirates (UAE), Kuwait, Saudi Arabia and Qatar.[34] They also include funds siphoned by al Qaeda from Islamic charities it has infiltrated[35] and general income from investments and businesses. Additional income is derived from credit card fraud that is estimated to raise approximately $12 million per year.[36] The strategic level retains access to all funds raised at this level. Accordingly, these sources of income contribute to al Qaeda's potential to buy and/or develop WMD. However, the sensitivity of these income streams to publicity suggests that they may be readily deterred if they can be identified. For example, many of the Arab benefactors prefer to remain anonymous. When identified, the actions of those donors should be highly publicized to deter further contributions.

After having raised funds, the organization's moneys need to be moved to fund operations around the world. To do this, al Qaeda makes extensive use of the informal hawala banking network.[37] The informal nature of this network means that it relies heavily on trust,[38] and therefore the hawala network may be susceptible to deterrence based on a campaign of undermining al Qaeda's financial credibility. For example, fraudulent transactions could be injected in a manner likely to cause participants sympathetic to terrorists to lose trust in the system and therefore be reluctant to do business with al Qaeda.

39

Additionally, law enforcement can play a deterrent role at this level of the al Qaeda organization. Take, for example, the recent case of Sami Amin Al-Arian, the University of South Florida college professor who was recently indicted with seven others accused of racketeering, abetting murder, extortion, money laundering, perjury, and immigration fraud.[39] Mr. Al-Arian is allegedly connected with and raises funds for the Palestinian Islamic Jihad, a Palestinian terrorist group responsible for the murders of over 100 people in the Middle East. Although he has not been tied directly to al Qaeda, arrests of this nature can put fundraisers on notice worldwide that the U.S. is tracking and arresting elements providing financial support to non-state actors who promote violence. These arrests and others like it must be leveraged to the maximum extent possible for their deterrent effect.

Tactical Level. Affiliated groups and cells conducting minor attacks at the tactical level are expected to be financially self-sufficient. Their sources of income include petty crime that has the unwanted side effect of potentially increasing the cell's visibility. While this visibility may assist a Defeat strategy, funds raised at this level are not believed to contribute to al Qaeda's capacity to buy and/or develop WMD. Therefore, deterrence of tactical financial operations is unlikely to contribute to deterring an al Qaeda WMD attack on the U.S. homeland.

4) Technical Capacity

Strategic Level. As previously mentioned, al Qaeda is known to have conducted research into chemical weapons and an artillery-based delivery method in Sudan. It is also known to have attempted to purchase uranium from criminal elements and to have hired an Egyptian nuclear scientist. States providing explicit support in the past for WMD research have included Sudan and Afghanistan. Sudan has been effectively deterred from hosting al Qaeda and its research since the assassination attempt on Mubarak,[40] and the post-Taliban regime in Afghanistan is opposed to al Qaeda and its WMD research. It is quite possible that al Qaeda had succeeded in developing WMD before the loss of its research facilities in Sudan and that it may still retain access to those weapons. This contention is consistent with bin Laden's claim to already have a WMD capability.[41] Given the infrastructure required to produce WMD, it appears deterrence might have an impact if these facilities can be identified and linked to al Qaeda. The Sudan attack serves as a precedent suggesting the potential for future action. Al Qaeda cannot dismiss the possibility of a future preemptive strike.

Operational and Tactical Levels. We have found no evidence of a technical capacity for developing WMD at the operational and tactical levels of al Qaeda.[42]

5) Operations Capacity

Strategic, Operational, and Tactical Levels.   The coordinated 9/11 attacks greatly exceeded the capabilities thought to be possessed by any terrorist organization at the time, and they were conducted in locations previously thought to be immune from successful terrorist attacks.[43] Furthermore, they demonstrated what has become an al Qaeda trademark, the use of suicide operatives to deliver synchronized mass casualty strikes.   Clearly, al Qaeda should be assessed as having the capacity to potentially deliver sophisticated attacks anywhere in the world.

Concerning al Qaeda's capacity for conducting effective information operations, we know that bin Laden has produced promotional material for television and the Internet using modern equipment[44] and that the al Jazeera satellite television station is the preferred media outlet.   The effectiveness of al Qaeda's media campaigns can be seen in opinion polls taken in 2002, suggesting that most Muslims living in the Middle East have been persuaded that al Qaeda was not responsible for the 9/11 attacks.[45]   Al Qaeda's willingness to use the modern media in a sophisticated fashion is further confirmed by bin Laden's pre-recording of videotapes to be broadcast during the allied campaign in Afghanistan.   Furthermore, observation of bin Laden's broadcasts shows that they are not only used for haranguing the West but also serve a vital process of reinforcing the ideological justification needed to persuade the foot soldiers to conduct what are otherwise regarded as un-Islamic tactics of using suicide bombers to kill civilians.

Al Qaeda's repeated use of religious justification for its goals and methods points to a weakness in its operational plans that might be used to undermine grassroots support.   By exposing ideological distortions, the U.S. may be effective in de-motivating, and thereby deterring, the operational and tactical components from employing this recruitment and motivational tool.   It will be essential for the U.S. and its allies to enlist moderate clerics of Islam to provide an alternative interpretation of the Koran when these distortions are espoused. A continued campaign of peaceful interpretations of Islamic teachings has the potential to deter the use of mass media to spread hatred, fear, and discontent.

Organization's Perception of U.S. Capability and Will

1) Past Behavior

Strategic, Operational, and Tactical Levels. Bin Laden frequently refers to the U.S. as a paper tiger, thereby demonstrating his belief that America has insufficient resolve to fight a protracted

and bloody campaign.   As assessed in Chapter 3, he cites the U.S. withdrawals from Vietnam, Somalia, and Lebanon as examples to prove that the U.S. will withdraw when faced with casualties. Hoffman suggests that bin Laden will continue in this belief despite the successful allied operations against Afghanistan after the 9/11 attacks. Bin Laden apparently believes that the Northern Alliance did most of the work in Afghanistan in much the same fashion that colonial Britain used native levies to fight those opposing its colony.[46]

Conversely, Gunaratna suggests the U.S. action in swiftly rounding up and extraditing a number of al Qaeda followers such as the Blind Sheikh after the 1993 attack on the World Trade Center "deterred further al Qaeda attacks in the U.S. in the second half of the 1990s." [47]   However, given what we know of bin Laden's capacity for strategic planning, it may also have been the case that al Qaeda was simply laying low while it regrouped and refined its field craft. Regrettably, the subsequent attacks on the Khobar Towers in 1996 and the U.S. embassy attacks in Kenya and Tanzania in 1998 undermine the argument that al Qaeda had been deterred.   Accordingly, one must conclude that past U.S. behavior, despite significant successes and demonstrations of resolve to commit ground forces to combat, has failed to deter al Qaeda at all levels.

2) Intelligence Capabilities

Strategic, Operational, and Tactical Levels. Al Qaeda's plans to bomb at least 12 U.S. embassies were thwarted by the U.S. as a result of monitoring al Qaeda's satellite phone conversations.[48]   Following publication of this monitoring, al Qaeda reverted to using person-to-person and highly encrypted Internet communications.[49] While these defeats denied al Qaeda some of its objectives, the subsequent 2002 attacks in Kenya and Indonesia (Bali, via JI) confirm that it has not been deterred from attacking U.S. and allied Western interests.   It is possible that what we have seen is a move away from targets in the U.S. homeland, because of its more effective Defend and Defeat strategies, and toward softer targets in more vulnerable countries.   However, this may simply be an attempt to buy time while al Qaeda adapts its field craft to the new conditions.   Given the long planning cycles used for al Qaeda attacks, it may be several years before we know if the system has been deterred from attacking targets on the U.S. homeland.   Accordingly, we should continue to assume al Qaeda intends attacking the U.S. homeland.

3) Defend Capabilities

Strategic, Operational, and Tactical Levels. Since the 9/11 attacks, the U.S. has made progress in improving national defenses against terrorists.   For example, a federal Department of

Homeland Security has been established to coordinate all aspects of domestic security relating to terrorist attacks. A Transport Security Authority has been established as part of this department to ensure a high standard of airport security while considerable research is being conducted, and measures put in place, to improve the security of seaports.   While these measures of themselves are unlikely to deter al Qaeda from attacks against U.S. interests, they can be expected to raise the cost of conducting complex attacks on the U.S. homeland and thereby encourage al Qaeda to become biased towards relatively simple attacks (i.e., non-WMD), outside the U.S. homeland.

To enhance their deterrent value, significant improvements to the defensive posture at home should be extensively publicized. For example, while the color-coded threat level system implemented by the Department of Homeland Security tends to make the American public anxious when threat level conditions are raised, it is likely to have a similar effect on a terrorist cell seeking to conduct a WMD attack. Highly visual improvements in security at airports, ports, and border crossings in the U.S. might be enough to dissuade a terrorist from taking action. At a minimum, such defenses will limit terrorist target sets. Even though these measures do not provide complete security, they might buy the country time and/or cause a nervous terrorist to make a mistake.

4) Defeat Capabilities

Strategic, Operational, and Tactical Levels. At the strategic level, the dramatic defeat of al Qaeda's Afghanistan base and the Taliban government that had supported it signifies the single most important success the U.S. has achieved in its war against al Qaeda.   Hoffman has suggested that bin Laden is unlikely to revise his view of the U.S. as being a paper tiger.   However, the display of resolve by coalition forces including many Islamic countries such as Pakistan and Turkey provides a powerful and highly credible precedent that may help deter potential state sponsors, Arab benefactors, technicians, and Islamic charities.

Individual successes at the operational and tactical level can also have a chilling effect on recruitment and morale. Such successes include foiling plans by JI to blow up embassies in Singapore, thwarting the attempt to blow up a passenger aircraft using a shoe bomb, the capture of bin Laden confidant Abu Zubaydah in Pakistan, and defeating a terrorist cell in London capable of producing the poison ricin.   The successful attack by a Predator unarmed aerial vehicle on suspected al Qaeda figureheads in Yemen linked to the bombing of the *USS Cole* in October of 2000, is possibly the most visible and useful attack on the tactical level of the organization to date.[50]   This act, while contributing

little to the overall defeat of the organization, has the potential from a deterrence perspective to undermine resolve of individual actors and reduce the scope of al Qaeda operations.

Ability of the Sides to Communicate

1) U.S. Capability to Communicate with the Organizational Component

　　Strategic, Operational, and Tactical Levels. When located, al Qaeda's leaders have either been captured or killed.   Similarly, direct communication between the U.S. and al Qaeda's leaders is difficult. Therefore, direct communication at the strategic level is problematic.   While the potential exists for the U.S. to communicate through third parties such as Iran or the Pakistani ISI, no evidence of this capacity exists at the unclassified level.   Accordingly, the principal means for communication with al Qaeda's leadership will need to be through public broadcasts and policy pronouncements in the hope that they will be transmitted to the leaders. From a technological standpoint, it is clear bin Laden has the capability to receive our signals via the open media. It is also both possible and desirable to discuss matters directly with states that might provide support to al Qaeda operations.   These communications must be pursued vigorously before taking direct action against al Qaeda assets within another state's boundaries.

　　Communications at the operational and tactical levels might be politically and technically more feasible. It is quite possible the U.S. could send a direct message to scientists, financiers, and logisticians providing support to al Qaeda at this level. In fact, merely stating "we know who you are and what you're up to" could have the desired deterrent effect.

2) Component's Ability to Receive Signals

　　Strategic, Operational and Tactical Levels.   Bin Laden's statement claiming that the current struggle is about religion, and refuting statements by President Bush and Prime Minister Blair that it is a war on terrorism,[51] confirms that he is clearly able to receive messages sent through the public media.   Furthermore, bin Laden's history of using press conferences such as the one held on May 26, 1998 to announce the formation of the World Islamic Front for the Jihad against the Jews and the Crusaders[52] confirms a clear capacity to transmit messages to the West.

Step 2 Summary

　　Except for states that sponsor or provide safe haven for al Qaeda operations, the Operational Level of the al Qaeda organization appears to be most susceptible to deterrence-based approaches. As

44

the ability to launch a successful WMD attack requires the management of a complex supply train, our analysis focused on several key links in the chain that may well be deterrable. These include wealthy benefactors, WMD scientists, infiltrated Islamic charities, and the hawala banking network. A strategy based on discrediting the religious credentials and justifications of al Qaeda's senior leaders may have significant success in deterring the nodes mentioned as well as some tactical components. We will develop such strategies in the next step.

Step 3: Strategize – Option Development and Implementation

Strategic Level

Step 2 of the SASM model revealed the following organizational weaknesses and implications for deterrence. The bullets below outline our recommended deterrence-based strategy:

- States suspected of being sympathetic to al Qaeda have return addresses and physical assets that they value. Accordingly, they must be put on notice that providing safe haven or technical assistance is tantamount to conducting the attack themselves. The new U.S. National Strategy to Combat Weapons of Mass Destruction takes the first step in defining this policy; however, deterrence should be given a more prominent role in the document.
  - o Past actions demonstrate that U.S. threats of intervention in states supporting al Qaeda have significant credibility.
  - o Recent activities in Afghanistan lend credibility to future U.S. threats aimed at preventing state actors from harboring or assisting al Qaeda.
- Counterproliferation measures are critical to hindering al Qaeda from acquiring WMD.

Operational Level

Our analysis of the operational component of the al Qaeda terrorist system suggests the following vulnerabilities and opportunities for successfully engaging the target component with deterrence-based strategies:

- Wealthy Arab benefactors represent potentially deterrable key elements at the operational level of the al Qaeda terrorist system. These individuals are identifiable, have homes and businesses worth maintaining, and in some cases have prominent positions within their political and social environments. Identifying and arresting key al Qaeda contributors and publicizing these events to maximize their deterrent effect can have an impact on future operations.

- Al Qaeda's reliance on religious indoctrination and justification suggests a susceptibility to deterrence at this level by information operations from credible and moderate Islamic religious figures discrediting al Qaeda's ideologies of Islamic teachings.

- Infiltrated Islamic charities channel donations to al Qaeda and assist with international money transfers. Because many of these charities have legitimate goals, they may be susceptible to deterrence by exposing their activities and by educating them about the errors in al Qaeda's ideology.

- Al Qaeda's savvy use of the media suggests that any information operations aimed at deterring their supporters will need to be very sophisticated. However, al Qaeda has already created an audience that is a ready-made target for a pro-Western media campaign.

- Successful Defeat and Defend operations result in objective denial causing the organization to reduce the scope of its operations or shelve plans entirely. Successes in these areas should be highly publicized and leveraged to the maximum extent possible to achieve deterrent value. Direct attacks on al Qaeda's operatives indirectly contribute to deterrence and will likely erode the morale of mid-level operators. Morale is affected when operatives witness unsuccessful operations. By the same token, highly visible defensive measures can force operatives to abort operations. The appearance of tight security or publication of technical systems aimed at detecting WMD entering the U.S. might cause the operatives to think twice about the operation, or they might induce a mistake. The U.S. should highly advertise its defensive capabilities to build on this perception of invulnerability.

- Cooperative Threat Reduction funding can be used to improve security at weapons storage areas within the confines of the former Soviet Union. Furthermore, this program should be expanded to secure materials in other countries that maintain fissionable materials and chemical/biological assets suitable for weaponization. The appearance of enhanced security at facilities will have a deterrent effect, thus persuading would-be terrorists from stealing weapons.

Tactical Level

Analysis of the tactical component of the system has identified the following weaknesses and potential deterrent strategies:

- Al Qaeda relies heavily on religious indoctrination and justification. Fundamental ideas and justification for the cause are even more important at this level. Deterring suicide bombers on WMD missions one person at a time is futile. One must attempt to undermine fundamental beliefs in order to have a credible impact on the general recruiting base of the population. If the cause can be discredited on a broad scale, al Qaeda will loose its capacity to recruit and obtain financial support.

- While understanding and seeking out solutions to the root causes of terrorism does not constitute traditional deterrence, efforts to improve standards of living fits within our concept of rewards and can erode support for radical behavior and moderate hatred toward the U.S. Any efforts in this vein should be highly publicized for their positive contribution to deterrence.

- Assist states with improving their border security and methods of monitoring travel by suspect individuals. Publicize system improvements and violations to deter unlawful entry into sovereign states.

Step 3 Summary

There is no silver bullet that can be aimed at any given level of the al Qaeda system to ensure success against a WMD attack. The operational level of al Qaeda appears to be most susceptible to deterrent strategies; however, at the strategic level, state sponsors represent another promising target for these approaches. Addressing the tactical level of the organization will require a broadly based, mass-media approach. It may be helpful to note that a ready-made audience exists for such a campaign as a result of al Qaeda's own media activities. The most difficult aspect of this problem may not be in determining the strategy, but in knowing, once the strategy is implemented, whether or not it is having the desired effect. Monitoring the al Qaeda response is addressed in Step 4 of the SASM model.

Step 4 – Monitor

Intelligence will be the key to determining whether or not the strategies identified in Step 3 of the model are having their desired effect. As strategies are devised in Step 3, one should also consider how effectiveness could be measured. Given the consequences of wrongly assuming that deterrence is working, the emphasis that the policymaker places on adopting a useful measure and the Intelligence

Community places on monitoring can mean the difference between the status quo or a mass casualty WMD event. We acknowledge that obtaining reliable data is going to be very difficult, if not impossible, in some cases; however, policymakers should not be discouraged from attempting to collect data to evaluate the effectiveness of deterrence strategies. Potential MOE for each level of al Qaeda are highlighted below:

Strategic Level Measures of Effectiveness

- **Measure Numbers and Levels of Violence Associated With Non-WMD Events**. An escalating number of non-WMD events should cause one to consider whether or not a given strategy is having the desired effect. Likewise, the magnitude of an event and the propensity to induce mass casualties should be cause for concern. While absence of terror does not preclude a WMD event, one can derive important trend information from al Qaeda activity.

- **Complexity and Organizational Coordination of Non-WMD Events.** Experts also measure the complexity and synchronization of operations. Increasingly complex operations signal a capability to handle the highly technical aspects and the degree of coordination a WMD attack would likely require. A reduction in the complexity and willingness to hit hard targets might similarly suggest a deterrent strategy was having the desired effect.

- **Communications Addressing WMD**. Open source communications of the intent to commit a WMD attack may be a signal that a given strategy is either taking hold or not. Possibly more important is the interception of covert traffic on the network suggesting a WMD strategy is being contemplated.

- **Interview Results of Captured Operatives.** The capture of Ramzi bin al-Shibh provides the perfect example of how captured terrorists can help us measure the capability and intent al Qaeda has with respect to WMD. According to the USA Today, he has provided inside information on the al Qaeda WMD program. Interrogations of al-Shibh have reportedly been "very productive" in uncovering al Qaeda's "nuke-bio-chem program." [53] Bin al-Shibh and other informants should be used carefully to discern the extent of the al Qaeda program.

- **Evidence of WMD Testing.** This is a clear signal of strategic intent. Leads indicating unusual outbreaks of disease or casualties in countries suspected of harboring terrorists should be investigated thoroughly. Similarly, testing could be visible through accidents and/or injuries.

48

Operational Level Measures of Effectiveness

- **Unusual Money Movements.** Movements of money between suspect fund raising companies, holding companies, charitable organizations, and prospective terrorist entities should be baselined and tracked for spikes in the curve. A flurry of money movement could signify an operation is imminent.

- **Changes in Black Market Component Price Levels.** Trends in prices of potential dual-purpose WMD materials and components should be tracked. For example, one should track the black market prices of fissile/radiological material, specialized chemical precursors, and biological agents. Increases in price levels might suggest the success of strategies directed at denying terrorists access to these materials.

- **Grossly Inflated and/or Deflated Prices of Specific Goods.** Al Qaeda is known to manipulate import and export prices as a means of moving money internationally. Significant variations in the market prices of commodities can be identified and possibly used to track al Qaeda money transfers.

- **Travel of Scientific and Logistical Operatives.** Movements of suspect scientists and logistical operatives should be baselined and tracked to the extent possible. Travel frequency and location can indicate suspect behavior.

- **Network Communications Levels.** This measure can apply to all levels within the organization. Traffic within and between levels of the organization should be monitored for trend data.

Tactical Level Measures of Effectiveness

- **Sentiment in the Local Community in Known Populations Supporting the Group.** This is a qualitative (as opposed to a quantitative) measure of effectiveness that is potentially useful in determining the likelihood of finding recruits for WMD attacks. It may also help the U.S. gauge al Qaeda's overarching popularity. Interviewing members of the general population can help measure changes in attitudes following efforts to address underlying causes of unrest and debunk radical religious teachings.

- **Numbers of Close Followers of Inflammatory Religious Leaders.** While inflammatory religious leaders may not have direct ties to al Qaeda, they are essential for the recruitment of

49

followers, and they also provide a performance measure for dissatisfaction with the current social, religious, and political order. Accordingly, numbers of followers can be used as a more quantitative measure of support for radical Islam.

The MOE listed above might apply to one or more levels within the organization and multiple deterrent strategies. They are listed above as either strategic, operational, or tactical measures to signify where they might be most applicable.

CASE STUDY SUMMARY

The following three tables consolidate our findings from Steps 3 and 4 of the al Qaeda case study. When combined, they comprise an illustrative overarching deterrence strategy with corresponding MOE.

Strategic Level Summary

TABLE 15: STEP 3 & 4 SUMMARY--STRATEGIC LEVEL

Deterrence Strategy	Best Response Authority	Measure Of Effectiveness
Directly contact suspect states and put them on notice that harboring or assisting al Qaeda to achieve WMD capabilities is tantamount to committing a WMD attack on the U.S. homeland	U.S. and Western Allies	Measure Numbers and Levels of Violence Associated With Non-WMD Events Complexity and Organizational Coordination of Non-WMD Events Communications Addressing WMD Interview Results of Captured Operatives Evidence of WMD Testing
Employ counterproliferation strategies when linkage between states possessing WMD and terrorist organizations is confirmed. Highly visible actions will have a deterrent effect. (Iraq will be a test case)	Entire U.N. Community led by U.S. military	Communications Addressing WMD Measure Numbers and Levels of Violence Associated With Non-WMD Events Complexity and Organizational Coordination of Non-WMD Events

Operational Level Summary

TABLE 16: STEP 3 & 4 SUMMARY--OPERATIONAL LEVEL

Deterrence Strategy	Best Response Authority	Measure Of Effectiveness
Identify wealthy Arab benefactors who support al Qaeda financially and highly publicize arrests of those individuals providing direct support and the seizure of assets	Middle East Allies, Intl Banking Community	Unusual Money Movements Changes in Black Market Component Price Levels Grossly Inflated and/or Deflated Prices of Specific Goods
Identify subversive/ al Qaeda infiltrated charitable organizations and highly publicize their arrests and seizure of assets	Middle East Allies, Intl Banking Community	Unusual Money Movements Changes in Black Market Component Price Levels Grossly Inflated and/or Deflated Prices of Specific Goods
Identify and track WMD scientists and logisticians, ensure they understand we know who they are and are watching their activities. Threaten reprisal should they provide material support to al Qaeda.	Western Allies	Travel of Scientific and Logistical Operatives Network Communications Levels
Enhance efforts to objectively deny terrorist organizations from obtaining WMD by providing additional funding for Cooperative Threat Reduction (CTR) and enhancing security of fissile, chemical, and biological materials. Highly publicize these efforts to maximize their deterrent effect.	Western funding focused on all states possessing WMD	Changes in Black Market Component Price Levels Network Communications Levels
Highly publicize defensive capabilities at home and advertise their capabilities abroad	U.S. media through Middle Eastern media outlets	Network Communications Levels Interview Results of Captured Operatives
Highly publicize U.S. Defeat successes abroad to serve as a deterrent to al Qaeda's other operatives	U.S. media through Middle Eastern media outlets	Network Communications Levels Interview Results of Captured Operatives
Establish and/or enhance use of Middle Eastern media outlets to promote or explain U.S. policies	U.S., Middle East Allies, governments of moderate Islamic countries	Sentiment in the Local Community in Known Populations Supporting the Group Numbers of Close Followers of Inflammatory Religious Leaders

Tactical Level Summary

TABLE 17: STEP 3 & 4 SUMMARY--TACTICAL LEVEL

Table 4.3		
Step 3 and 4 Summary—Tactical Level		
Deterrence Strategy	**Best Response Authority**	**Measure Of Effectiveness**
Enlist moderate clerics to challenge the teachings of radical/militant Islamic leaders and provide their commentary in mass media outlets	Middle East Allies	Sentiment in the Local Community in Known Populations Supporting the Group Numbers of Close Followers of Inflammatory Religious Leaders
Highly publicize U.S. efforts to address the root causes of terrorism and improve political processes and economic conditions	U.S., Middle East Allies, governments of moderate Islamic countries	Sentiment in the Local Community in Known Populations Supporting the Group Numbers of Close Followers of Inflammatory Religious Leaders
Assist moderate states with enhanced methods to control borders and monitor travel between states and publicize arrests and violations in the Arab press	U.S., Middle East Allies, governments of moderate Islamic countries	Travel of Scientific and Logistical Operatives

[1] Paul D. Davis and Brian Michael Jenkins, *Deterrence & Influence in Counterterrorism* (Santa Monica, Calif: RAND, 2002) 22.

[2] Barry R. Posen, "The Struggle against Terrorism: Grand Strategy, Strategy, and Tactics," *International Security* 26.3 (2001-2002) 43.

[3] H. Mir, "Osama Claims he has Nukes: If US uses N-arms it will get same Response," *Dawn Newspaper Group* 10 Nov. 2001, 8 Jan. 2003 <http://www.dawn.com/2001/11/10/top1.htm>.

[4] Mir.

[5] Rohan Gunaranta, *Inside Al Qaeda: Global Network of Terror,* (New York: Columbia University Press, 2002) 47.

[6] "Ricin as a weapon," 8 Jan. 2003 <Http://www.cnn.com/2003/WORLD/europe/01/07/terror.poison.extremists/index.html>.

[7] Gunaratna 157.

[8] Gunaratna 21.

[9] Gunaratna 23.

[10] N. MacFarquhar and J. Rutenberg, "A Nation Challenged: The Video; Bin Laden, in a Taped Speech, Says Attack in Afghanistan are a War Against Islam," *The New York Times* 4 Nov. 2001. <http://query.nytimes.com/gst/abstract.html?res=FA0B14FE3F5D0C778CDDA80994D9404482>.

[11] Gunaratna 230.

[12] Bruce Hoffman, "Lessons of 9/11," Joint Inquiry Staff Request (Washington DC: RAND, 8 Oct. 2002) 16.

[13] Gunaratna 235.

[14] Gunaratna 57.

[15] Ministry of Home Affairs of Singapore, *White Paper: The Jemaah Islamiyah Arrests and the Threat of Terrorism* (Singapore: 7 Jan. 2003) 12.

[16] Hoffman, "Lessons of 9/11" 11.

[17] Gunaratna 79.

[18] Gunaratna 10.

[19] Gunaratna 56-57.

[20] Gunaratna 57.

[21] Gunaratna 57.

[22] Brad Roberts, "Terrorist Campaigns: What Can Deterrence Contribute to the War on Terror?" MIT Center for International Studies Seminar, 292 Main St, Cambridge, Mass., 26 Feb. 2003.

[23] Gunaratna 16.

[24] Gunaratna 31.

[25] Gunaratna 32.

[26] Gunaratna 61.

[27] Gunaratna 146.

[28] Gunaratna 40.

[29] Gunaratna 211.

[30] Rina Amiri, personal interview, 7 Jan. 2003.

[31] Gunaratna 61.

[32] D.K. Kartchner, personal interview, 18 Dec. 2002.

[33] Gunaratna 61.

[34] Gunaratna 60-62.

[35] Gunaratna 60-62.

[36] Gunaratna 65.

[37] Gunaratna 63.

[38] Phillip Williams, "Financing Terrorism," Whitehead Center for International Affairs Seminar, Harvard University, Cambridge, Mass., 14 Nov. 2002.

[39] Eric Lichtblau and Judith Miller, "Threats and Responses: The Money Trail; Indictment Ties U.S. Professor to Terrorist Group," *The New York Times* 21 Feb. 2003 A.1.

[40] Gunaratna 160.

[41] MacFarquhar and Rutenberg.

[42] While in this case study we have found no evidence of a WMD technical capacity at the tactical and operational levels of alQaeda, it is possible that a strategic capability can become available to lower levels of the organization in a short period of time. For example, instructions on how to manufacture ricin could be developed at the strategic level and then implemented at the operational or tactical level.

[43] Hoffman, "Lessons of 9/11" 6.

[44] Gunaratna 10-11.

[45] Gunaratna 52.

[46] Hoffman, "Lessons of 9/11" 16.

[47] Gunaratna 102.

[48] Gunaratna 163.

[49] Gunaratna 80.

[50] Rowan Scarborough, "U.S. Kills al Qaeda Terrorist Who Attacked Cole," *The Washington Times* 5 Nov. 2002 A1.

[51] MacFarquhar and Rutenberg.

[52] Gunaratna 47.

[53] Tony Locy and Kevin Johnson, "Suspect Helping U.S. Gauge al-Qaeda's Arsenal," *The USA Today* 15 Jan. 2003 A4.

CHAPTER 5: FINDINGS AND RECOMMENDATIONS

Once a terrorist organization is deemed to posses a potential WMD threat, national security policymakers must quickly determine the priority to be allocated to Deter, Defend, and Defeat strategies. Reliance upon traditional heuristic methods risks exposing the U.S. community to potentially avoidable attacks and ties the policymaker to a limited set of Defend or Defeat options. While conventional wisdom suggests terrorists cannot be deterred, our analysis convinces us deterrence-based strategies are not given sufficient credit and can contribute to protecting the U.S. homeland from a WMD attack. Key findings and recommendations are outlined below.

Findings:

- **Deterrence can play a significant role in preventing a WMD attack on the U.S. homeland.** There are a set of options, short of defending the entire U.S. and defeating all terrorist threats that have the potential to add considerable value. These approaches do not presently appear to be fully reflected in current national security policy.

- **The SASM model presents policymakers with a structured framework with which to assess the feasibility of identifying measures that may serve to deter a terrorist WMD attack on the U.S. homeland.** By applying the four steps of the model, policymakers may be able to discover vulnerable components of a terrorist system which, when deterred, may deter the entire organization for at least some period of time. In the very least, the model confirms for policymakers that deterrence is not an option and that their best option to prevent a WMD attack is to pursue more costly and elaborate Defend and/or Defeat measures.

- **When contemplating deterrent-based strategies, it is essential to break the target terrorist network into its strategic, operational, and tactical levels.** One should <u>not</u> consider the organization as a homogeneous entity but rather as a system of interdependent components operating at strategic, operational, and tactical levels. The one-size-fits-all approach is too coarse to apply within this context.

- **Some components may be responsive to deterrent strategies while others within the organization may not.** Component attributes helping to determine if deterrent strategies may be effective include:
  - ➢ A coherent and identifiable command and control structure
  - ➢ Elements of the network such as benefactors who have tangible assets that are of value and can be targeted
  - ➢ Reliance on another state or element within the organization for technical, political/diplomatic, logistical, or financial support or safe haven
  - ➢ Requirement for general support as well as trust between members to cement internal relations and motivations
- **Deterring one or more critical components of a terrorist system at one level could be enough to deter the entire network.** It may not be necessary to attempt to deter an entire terrorist organization from using WMD. There are likely to be several key nodes within the network that have vulnerabilities susceptible to exploitation. Once identified, the U.S. could target these vulnerable components with different means to convince them that it is not in their interest to pursue a WMD attack against the U.S. Through such action, it may be possible to deter the entire terrorist system for at least some period of time. It seems that the greatest chances for success for applying these levers would be with state sponsors at the strategic level and in general at the operational level.
- **Defend, Defeat, and Deter strategies overlap to some extent and are mutually reinforcing.** Aspects of a defensive posture and offensive operations will have a deterrent effect. For example, the allied anti-Taliban campaign in Afghanistan will have a long-term deterrent effect on other states providing safe haven or harboring terrorist networks. Likewise, the presence of highly effective defensive measures will have a deterrent impact. To leverage the full effect of defeat successes and defensive measures, they must be highly publicized and advertised in multiple venues.
- **The SASM model provides the policymaker with a rigorous framework that can be used to evaluate deterrent-based strategies.** While the model does not predict the outcome of any one approach, it offers an architecture to assess capabilities, develop options,

and measure success. This type of methodical approach is presently missing from the literature.

Recommendations:

As a result of this research, our study group is convinced the SASM model can effectively determine the contribution deterrence can make to prevent a WMD attack on the U.S. homeland. We strongly urge the NSC to direct the Department of Defense (DoD) to lead an interagency effort aimed at implementing the SASM methodology. While DoD is arguably best suited to lead this effort, the Department of State, the Department of Homeland Security, and the Intelligence Community should play major roles. This interagency group should incorporate classified material, formalize the strategy evaluation process, and further refine the framework. Additionally, the Intelligence Community should consider terrorist organizations other than al Qaeda as part of this study. Our research suggests Aum Shinrikyo, Hezbollah, and Jemaah Islamiyah might also pose a WMD threat to the U.S. Other groups, beyond the four organizations listed above, might be added in accordance with Intelligence Community recommendations.

Furthermore, we recommend adding a fourth pillar entitled "Deterrence" to the "National Strategy to Combat Weapons of Mass Destruction" to reflect more accurately the value deterrence can bring to the war on terrorism.[1] In this document the White House does not place "Deterrence" on equal footing with the three pillars of its national strategy: 1) Counterproliferation, 2) Non-proliferation, and 3) Consequence Management. Deterrence is listed in the document as a subset of the Counterproliferation pillar. We feel this misrepresents the meaning of both counterproliferation and deterrence and devalues the contribution deterrence-based strategies can make.

Finally, while we have conducted a comprehensive discussion of this topic, by no means have we exhausted the subject. Accordingly, a number of areas worthy of follow-on research are discussed in Appendix 2.

---

[1] National Strategy to Combat Weapons of Mass Destruction, Washington, D.C.: The White House, Dec. 2002: 1-6.

APPENDIX 1 - SASM MODEL QUESTIONNAIRE

STEP 1: SCREEN--IS THE ORGANIZATION OF INTEREST?

Intent
1. Could the organization perceive a benefit or achieve a known goal by employing WMD on the U.S. homeland?
2. Has the organization stated a desire to acquire or employ WMD?

Capability
1. Does the organization have the technical capacity to employ WMD?
2. Is there evidence of efforts to acquire WMD capability?

STEP 2: ANALYZE--IS THIS LEVEL OF THE ORGANIZATION DETERRABLE?

U.S. Analysis of the Organizational Component

1. Goals and Ideology

   a. What are the vision, and purpose of the component?
   b. Is the component religiously motivated?
   c. Is self-preservation of the component essential to itself or the larger organization?
   d. How committed to the cause is this component of the organization?

2. Network Structure

   a. Does the component have a coherent command and control structure and how does it receive direction from higher levels of the leadership chain?
   b. How much of the command and control structure is horizontally distributed?
   c. How does it communicate with lower levels of the leadership chain?
   d. Do targetable elements exist?
   e. Do we know who the leaders of the component are and where they're based?
   f. Do these leaders have the authority and control to launch or abandon operations by subordinate cells?
   g. How dispersed geographically is this component of the organization?

3. Financial Structure

   a. What are the sources of the component's income?
   b. Does the component generate/contribute sufficient funds to develop WMD?
   c. Does the component generate/contribute sufficient funds to purchase WMD?

4. Technical Capacity

   a. Does the component have a scientific infrastructure capable of independently weaponizing WMD?
   b. Is the component dependent on external technical expertise?
   c. Has the component received WMD materials/items from another state?
   d. Has the component received WMD materials/items from a non-state entity?
   e. Are we aware of any WMD testing?

5. Operations Capacity
   a. Does this component of the organization have a record of novel attack methods?
   b. Is there an increasing pattern of lethality or indifference to the scale of casualties involved in past actions?
   c. Does the component have a history of committing suicide attacks?
   d. Has the component conducted, coordinated, and synchronized operations with other organizational components?
   e. Does the component have an effective means of conducting information operations?
   f. Are there essential and identifiable training facilities tied to this level of the organization?

Organization's Perception of U.S. Capability and Will

1. Past Behavior

   a. Has the U.S. or its allies directed action against this component of the organization in the past? Was it effective?
   b. Has the U.S. acted against states supporting the target organizational level? Was it effective?
   c. Has the U.S. successfully acted against other states or terrorist groups in a way that could serve as a "lesson?"
   d. Has the U.S. successfully led an international coalition in response to terrorist threats?
   e. Has the U.S. articulated a clear doctrine regarding WMD use on the U.S. Homeland since the end of the Cold War? Has this message been consistently translated by all levels and branches of government?
   f. Has the U.S. conducted information operations/public diplomacy convincing to the terrorist organization's bases of support?

2. Intelligence Capabilities

   a. Does the organizational component believe the U.S. Intelligence Community has the capability to anticipate its operations?
   b. Has the U.S. disrupted previous activities on the basis of accurate and timely intelligence?
   c. Has the U.S. effectively coordinated intelligence operations and shared intelligence information with other countries?

d. Has the organizational component modified its modus operandi as a result of U.S. Intelligence activities?

3. Defend Capabilities

a. To what degree have U.S. defensive measures dissuaded terrorists from pursuing a WMD strategy against the U.S. homeland?
b. To what degree has the international community dissuaded terrorists from pursuing a WMD strategy?
c. What is the cost to the organization should a WMD attack on the U.S. homeland be foiled, in terms of: prestige? initiative? support?

4. Defeat Capabilities

a. Are there credible threats the U.S. can communicate?
b. Does the U.S. have the political will to use them?
c. What are the costs to delivering on the threat?
d. What are the costs associated with taking no action?

Ability of the Sides to Communicate

1. U.S. capability to communicate with the organizational component

a. Can the U.S. Government communicate unambiguously with this component of the organization?
b. Can the U.S. Government communicate with a state or non-state actor who has the ability to communicate with the target component?

2. Component's ability to receive signals from the U.S.?

a. Can the component receive and comprehend intended messages from the U.S. Government?
b. Does the component have the ability to communicate unambiguously with the U.S. Government?

STEP 3: STRATEGIZE--OPTION DEVELOPMENT AND IMPLEMENTATION

1. What are the key vulnerabilities of this component of the target organization?

2. What vulnerabilities can the U.S. successfully influence?
   a. Military (e.g., operations, train host nation counter-terrorist forces)

   b. Economic (e.g., freezing assets, funding counter-terror campaigns)

   c. Political/Diplomatic (e.g., counter-terror coalition building)

60

    d. Legal (e.g., bringing terrorists to justice, strengthening laws)

    e. Information Operations (e.g., fracturing organizational cohesion, isolating leadership,

    f. inciting mistrust, prying away public support, molding/mobilizing world opinion)

3. Where else can the U.S. derive support for its policies?
    a. UN

    b. Allies

    c. Regional organizations

    d. Non-state actors such as non-governmental organizations (NGOs)

    e. World opinion

4. What are the organizational component's capabilities to respond?

STEP 4: MONITOR—EVALUATE OPTION EFFECTIVENESS

1. Have the intent and capability of the organizational component changed sufficiently to merit re-screening?
2. Has the component of the organization responded positively to the deterrent strategy?
3. Are there measures of effectiveness available to determine success or failure?
4. What are the measures of effectiveness that should be continuously evaluated?

APPENDIX 2 - QUESTIONS FOR FURTHER RESEARCH

While our effort reflects a serious attempt to study the impact deterrence can have on preventing a WMD attack on the U.S. homeland, we did not completely exhaust this research topic. Questions listed below might serve as the launching point for further study:

- Does the U.S. government do enough to maximize publicity given to offensive and defensive victories to leverage their deterrent effect? How can we better exploit successful interdiction operations, the capture of key interlocutors, and defensive practices to direct terrorists away from WMD-related options?

- What other steps can the Intelligence Community take to actively monitor terrorist organizations and devise sound Measures of Effectiveness? What are the critical indicators predicting WMD attacks?

- Does the U.S. government do enough to pronounce a clear, credible, and consistent declaratory policy highlighting the catastrophic consequences a terrorist organization will incur should it employ WMD? Should this policy apply equally to any state that provides support or safe haven to a terrorist network? Is this policy communicated to all levels of the target organization (strategic, operational, and tactical)?

- Does the U.S. have sufficient capability to attribute WMD attacks credibly and graphically to the sponsoring terrorist organization? Can we use such attribution to undermine popular support for the terrorists' cause?

- Should the U.S. hold any state intentionally or inadvertently losing control of material contributing to a WMD attack accountable for its action or inaction? In the case of inadvertent loss of material, what steps should or can be taken?

GLOSSARY

FROM THE DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS AS AMENDED THROUGH 14 AUGUST 2002.

Anti-terrorism

Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

Counterterrorism

Offensive measures taken to prevent, deter, and respond to terrorism. Also called CT.

Deterrence

The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction.

Mass Casualty

Any large number of casualties produced in a relatively short period of time, usually as the result of a single incident such as a military aircraft accident, hurricane, flood, earthquake, or armed attack that exceeds local logistic support capabilities.

Measures of Effectiveness

Tools used to measure results achieved in the overall mission and execution of assigned tasks. Measures of effectiveness are a prerequisite to the performance of combat assessment. Also called MOEs. See also combat assessment; mission.

Terrorism

The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Terrorist Groups

Any element, regardless of size or espoused cause, that commits acts of violence or threatens violence in pursuit of its political, religious, or ideological objectives.

Weapons of Mass Destruction

Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon. Also called WMD.

WORKS CONSULTED

Allison, Graham. "Could worse be yet to come?" *The Economist* 361.8246 (2001): 19-21.

---. "Preventing Nuclear Terrorism." MIT Center for International Studies Seminar. 292 Main St, Cambridge, Mass. 4 Dec. 2002.

Allison, Graham and Kokoshin, Andrei. "The New Containment: An Alliance Against Nuclear Terrorism." *The National Interest* 69 (2002): 35-43.

Allison, G. T. and Zelikow, P. *Essence of Decision: Explaining the Cuban Missile Crisis.* New York: Longman, 1999.

Amiri, Rina. Personal interview. 7 Jan. 2003.

Anderson, William; Burrows, Mat; Forbes, Nancy; Gordon, David; and Hildebrand, Aaron. "Combatting Terrorism: Long- and Short-Term Strategies." Harvard University Seminar. JFK School of Government, Cambridge, Mass. 3 Mar. 2003.

Barnett, Tom. "Where–Not When–Preemption Makes Sense." *Transformation Trends – 18 November.* U.S. Department of Defense. Arlington, Virginia: 2002.

Benjamin, Daniel. "A Failure of Intelligence: Press, Politics and the Dawn of the Age of Sacred Terror." Harvard University Seminar. JFK School of Government, Cambridge, Mass. 9 Dec. 2002.

Bergen, P. L. "Picking Up the Pieces; What We can Learn From – and About- 9/11." *Foreign Affairs* 81.2 (2002): 169-175.

Betts, R. K. "Fixing Intelligence." *Foreign Affairs* 81.1 (2002): 43-59.

Bhopal: Chronology as of November 2002. 23 Jan. 2003. <http://www.bhopal.com/chrono.htm>.

Bowen, Wyn Q. "Deterring Mass-Casualty Terrorism." *Joint Forces Quarterly* 31 (2002): 25-29.

Brodie, Bernard. "The Anatomy of Deterrence." Santa Monica, Calif: RAND, 23 Jul. 1958.

Bunn, Matthew. "Commentary – A Nuclear Weapon Just Waiting to Happen." *The Los Angeles Times* 29 Aug. 2002: B17.

Campbell, Kurt M. and Flournoy, Michèle A. *To Prevail.* Washington, DC: The CSIS Press, 2001.

Carter, Ashton; Deutch, John; and Zelikow, Philip. "Catastrophic Terrorism: Tackling the New Danger." *Foreign Affairs* 77.6 (1998): 80-94.

Carter, Ashton B. Personal interview. 26 Nov. 2002.

Corn, G.S. and Aldykiewicz, J.E. "New Options for Prosecuting War Criminals in Internal Armed Conflicts." *Parameters* 32.1 (2002): 30.

Davis, Paul. Personal interview. 14 Jan. 2003.

Davis, Paul D. and Jenkins, Brian Michael. *Deterrence & Influence in Counterterrorism.* Santa Monica, Calif: RAND, 2002.

Dershowitz, Alan M. *Why Terrorism Works.* New Haven, Conn. and London: Yale University Press, 2002.

Falkenrath, Richard A. "Confronting Nuclear, Biological and Chemical Terrorism." *Survival* 40.3 (1998): 43-65.

Flynn, S. E. "America The Vulnerable." *Foreign Affairs* 81.1 (2002): 60-75.

Fuller, G. E. "The Future of Political Islam." *Foreign Affairs* 81.2 (2002): 48-60.

Gray, C. S. "Thinking Asymmetrically in Times of Terror." *Parameters* 32.1 (2002): 5.

Gunaranta, Rohan. *Inside Al Qaeda: Global Network of Terror.* New York: Columbia University Press, 2002.

Guthe, Kurt and Martinage, Robert. Personal interview. 15 Jan. 2003.

Hart, Gary and Rudman, Warren. "Beyond the Department of Homeland Security: Politics, Bureaucrats, & The War on Terrorism." Harvard University Seminar. JFK School of Government, Cambridge, Mass. 23 Sep. 2002.

Hoffman, Bruce. "Lessons of 9/11." Joint Inquiry Staff Request. Washington DC: RAND, 8 Oct. 2002.

---. "Re-Thinking Terrorism in Light of a War on Terrorism." Testimony before the Subcommittee on Terrorism and Homeland Security, House Permanent Select Committee on Intelligence, U.S. House of Representatives. Washington, DC: RAND, 26 Sep. 2001.

---. Personal interview. 15 Jan. 2003.

Hoffman, D. "Beyond Diplomacy." *Foreign Affairs* 81.2 (2002): 83-95.

Howard, M. "What's In A Name?: How to Fight Terrorism." *Foreign Affairs* 81.1 (2002): 8-13.

Hudson, Rex. A. "The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why?" Washington, DC: Library of Congress, Sep. 1999.

Indyk, M. "Back to the Bazaar." *Foreign Affairs* 81.1 (2002): 75-88.

Ivanchishin, Alexander F.; Fuller, Jeffrey D.; Sinai, Dr. Joshua; and Mann, Jennifer. Personal
interview. 20 Dec. 2002.

Jenkins, Brian Michael. *Countering al Qaeda*. Santa Monica, Calif.: RAND, 2002.

---. "Will Terrorists Go Nuclear?" P-5541. Santa Monica, Calif.: RAND, Nov. 1975.

---. "Terrorism: Current and Long Term Threats." Testimony before the Senate Armed Services
Subcommittee on Emerging Threats, U.S. Senate. Santa Monica, Calif.: RAND, 15 Nov.
2001.

Jervis, Robert; Lebow, Richard Ned; and Stein, Janice Gross. *Psychology and Deterrence*. Baltimore and
London: The Johns Hopkins University Press, 1985.

Kamp, Karl-Heinz; Pilat, Joseph F.; Stern, Jessica; and Falkenrath, Richard A. "WMD Terrorism: An
Exchange." *Survival* 40.4 (1998/1999): 168-183.

Kartchner, Dr. Kerry M. Personal interview. 18 Dec. 2003.

Kaufmann, William W. *The Requirements of Deterrence*. Princeton, New Jersey: The Center of
International Studies, 15 Nov. 1954.

Lavoy, Peter R.; Sagan, Scott D.; and Wirtz, James J., ed. *Planning the Unthinkable: How New Powers Will
Use Nuclear, Biological, and Chemical Weapons*. Ithaca, New York and London: Cornell University
Press, 2000.

Lichtblau, Eric and Miller, Judith. "Threats and Responses: The Money Trail; Indictment Ties U.S.
Professor to Terrorist Group." *The New York Times* 21 Feb. 2003: A.1.

Locy, Toni and Johnson, Kevin. "Suspect Helping U.S. Gauge al-Qaeda's Arsenal." *The USA Today*
15 Jan. 2003: A4.

MacFarquhar, N. and Rutenberg, J. "A Nation Challenged: The Video; Bin Laden, in a Taped
Speech, Says Attack in Afghanistan are a War Against Islam." *The New York Times*
<http://query.nytimes.com/gst/abstract.html?res=FA0B14FE3F5D0C778CDDA80994D94
04482>. 4 Nov. 2001.

McRaven, William H. Personal interview. 18 Dec. 2002.

Mellor, Brigadier William and Vaughn, Bruce. Personal interview. 17 Dec. 2002.

Ministry of Home Affairs of Singapore. *White Paper: The Jemaah Islamiyah Arrests and the Threat of
Terrorism.* Singapore: 7 Jan. 2003.

Mir, H. "Osama Claims he has Nukes: If US uses N-arms it will get same Response." *Dawn Newspaper Group* 10 Nov. 2001. 8 Jan. 2003 < http://www.dawn.com/2001/11/10/top1.htm>.

National Strategy to Combat Weapons of Mass Destruction. Washington, D.C.: The White House, Dec. 2002.

Netanyahu, Benjamin. *Fighting Terrorism.* New York: Farrar, Straus, and Giroux, 1995.

Parachini, P. A. and Cragin, Kim. Personal interview. 19 Dec. 2002.

Payne, Keith. *The Fallacies of Cold War Deterrence.* Lexington, Kentucky: The University Press of Kentucky, 2001.

---. Personal interview. 22 Nov. 2002.

Platt, James and Cave, Richard. Personal interview. 19 Dec. 2002.

Posen, Barry R. "The Struggle against Terrorism: Grand Strategy, Strategy, and Tactics." *International Security* 26.3 (2001-2002): 39-55.

Post, Jerrold M.; Ruby, Keven G. and Shaw, Eric D. "The Radical Group in Context: 1. An Integrated Framework for the Analysis of Group Risk for Terrorism." *Studies in Conflict & Terrorism* 25. (2002): 73-100.

---. "The Radical Group in Context: 2. Identification of Critical Elements in the Analysis of Risk for Terrorism by Radical Group Type." *Studies in Conflict & Terrorism* 25 (2002): 101-126.

Powers, Michael J. "Deterring Terrorism with CBRN Weapons: Developing a Conceptual Framework." *CBACI Occasional Paper 2.* Washington D.C.: Feb. 2001.

Presidential Decision Directive 39. "U.S. Policy on Counterterrorism." Washington, D.C.: The White House. 21 Jun. 1995. <http://www.fas.org/irp/offdocs/pdd39.htm>.

Quillen, C. "Posse Comitatus and Nuclear Terrorism." *Parameters* 32.1 (2002): 60.

Radio Australia. *APEC: Economic Consequences of Terrorism,* 27 Feb. 2003. <http://www.abc.net.au/ra/asiapac/programs/s793689.htm>.

"Ricin as a weapon," 8 Jan. 2003 <Http://www.cnn.com/2003/WORLD/europe/01/07/terror.poison.extremists/index.html>.

Roberts, Brad. "Terrorist Campaigns: What Can Deterrence Contribute to the War on Terror?" MIT Center for International Studies Seminar, 292 Main St, Cambridge, Mass. 26 Feb. 2003.

Scarborough, Rowan. "U.S. Kills al Qaeda Terrorist Who Attacked Cole." *The Washington Times* 5 Nov. 2002: A1.

Simon, Steven and Benjamin, Daniel. "America and the New Terrorism." *Survival* 42.1 (2000): 59-75.

Snyder, Glenn H. *Deterrence and Defense*. Princeton, New Jersey: Princeton University Press, 1961.

Stern, Jessica. *The Ultimate Terrorists*. Cambridge, Mass.: Harvard University Press, 1999.

---. Personal interview. 11 Dec. 2002.

Susser, E. S; Herman, D. B; and Aaron, B. "Combating the Terror of Terrorism." *Scientific American* 287.2 (2002): 70-77.

Teitel, Katie, Danis, Aaron, and Van De Velde, James. Personal interview. 17 Dec. 2002.

Williams, Phillip. "Financing Terrorism." Whitehead Center for International Affairs Seminar. Harvard University, Cambridge, Mass., 14 Nov. 2002.