

REPORT

February 2006

INDEPENDENT TASK FORCE
ON IMMIGRATION
AND AMERICA'S FUTURE

COUNTERING TERRORIST MOBILITY: Shaping an Operational Strategy

Susan Ginsburg

Former Senior Counsel and Team Leader,
National Commission on Terrorist Attacks Upon
the United States (9/11 Commission)



MIGRATION POLICY INSTITUTE

COUNTERING TERRORIST MOBILITY: Shaping an Operational Strategy

Susan Ginsburg

Former Senior Counsel and Team Leader,
National Commission on Terrorist Attacks
Upon the United States (9/11 Commission)

© 2006 Migration Policy Institute. All rights reserved. No part of this publication may be reproduced or transmitted in any form, or by any means, without prior permission, in writing, from the Migration Policy Institute.

TABLE OF CONTENTS

Executive Summary	1
Introduction	8
I. Defining Terrorist Mobility	18
II. Purposes of a Strategy for Constraining Terrorist Mobility	24
III. Elements of a Terrorist Mobility Strategy	27
A. Foundation: Terrorist Mobility Knowledge	28
B. Targeting: Terrorists Who Act as Travel Facilitators	46
C. Crime Control: Attacking Illicit Travel Networks	47
D. Global Awareness: Tracking Terrorists <i>En Route</i>	54
E. Border and Immigration Management: Securing Legal Entry Channels	59
F. Perimeter Control: Denying Access Through Illegal Entry Channels	70
G. Domestic Security: Constraining Terrorist Mobility in the United States	80
H. Recovery: Post-incident Terrorist Mobility Reviews	95
IV. Direction, Management, and Organization of a Terrorist Mobility Strategy	96
A. Obstacles to Effective Management and Organization	98
B. The National Security–Immigration Divide	102
C. New Arrangements to Attack Terrorist Mobility	105
V. National Strategic and Statutory Framework	116
Conclusion	126

COUNTERING TERRORIST MOBILITY

EXECUTIVE SUMMARY

The year 2006 is expected to be a time of substantial political debate on immigration and border management. Improving border security was a primary concern behind the establishment of the Department of Homeland Security (DHS), in response to the apparent ease with which terrorists entered the United States to plan for and carry out the 9/11 terrorist attacks. Now the topic of border management is at the center of the political debate on immigration reform. This is occurring at a time when national counterterrorism strategy itself is being updated, and a strategy for constraining terrorist mobility will be forthcoming from the National Counterterrorism Center (NCTC). These circumstances create a need and a valuable opportunity to examine how counterterrorism strategy relates to border security and immigration reform, and how terrorist mobility should be countered.

The first step is to recognize that while public discourse tends to equate blocking terrorists' ability to travel with immigration reforms, terrorist *mobility* comprises a set of problems distinct from, although clearly linked to, the phenomenon of global migration and the problem of controlling immigration to the United States. Solving the domestic immigration problem requires a democratic consensus about the level and criteria for immigration, taking into account the economic, social, and political forces that drive immigration. It means striking a balance among competing concerns over national cohesion, economic impact, a spectrum of human rights issues, compassion toward refugees, attacking human trafficking, and maintaining constitutional order. The balance of social unity, prosperity, and justice matters immensely to the country's security and legitimacy.

Prevailing over enemies that use terrorist stratagems, however, compels the United States to focus on small elusive groups and individuals who circulate globally and whose agenda is to kill citizens and damage infrastructure to force changes in US policy. Both migration, with its large-scale movements and periodic eruptions, and terrorism, with its devastating attacks, demand long-term responses. But migration of the

many and terrorism by a few must first be distinguished before the most effective policies and tactics against terrorism can be developed. That some of these will overlap in practice does not lessen the need for separately considered approaches and measures of success.

Thus, the second step toward improving our ability to constrain terrorist movements is to establish terrorist mobility fully and formally as a distinct functional component of counterterrorism. It should be viewed as analogous to our approach to terrorist finance and should elicit the same kind of broad attention from thinkers and practitioners. As a subfield of counterterrorism, terrorist mobility encompasses the study of terrorist movements, and how to both counter and exploit them.

The nature of terrorist movement can best be described in response to a series of key questions:

- How is the terrorist travel function managed—by a travel facilitator or by arrangements with illicit travel organizations?
- What are the global geographic routes and transportation practices?
- What are the illegal entry and residence tactics in the United States—both the legal channels used illegally and the illegal channels?
- What are the geographic variations in the use of legal and illegal channels?
- How do terrorists interact with the illicit travel infrastructure that supports migration outside legal channels and crime?
- What are the legal and cultural safeguards that nations and peoples develop for immigration and citizenship and other political or social factors that may inhibit or support terrorist mobility?

A terrorist mobility strategy (TMS) has three broad purposes:

- *Defensive*—securing transportation, entry, and immigration channels against undetected terrorist movements and against attacks;
- *Offensive*—exploiting the potential exposure created by terrorists' need to move people and material to disrupt them; and
- *Deterrent*—raising the risk of movement so far that it becomes a factor in dissuading terrorists from attack.

Most policy discussion has focused on the first, defensive homeland security purpose. And indeed, conceptually and practically, the three purposes overlap. For instance, an active defense by US border authorities does not passively await the approach of a terrorist or rely on hardened perimeters. Instead, it seeks to dismantle criminal travel networks through transnational criminal investigations; to reduce the vulnerability of legal travel channels through global efforts to raise travel document security standards; and to support the offensive tracking of individual terrorists using intelligence, border inspections and information analysis, among other actions.

The continued threat from Islamist terrorist groups is the obvious justification for a terrorist mobility strategy today. The mobility tactics used by Al Qaeda and its predecessors in the successful 9/11 attack and previous attacks against Americans in the United States and abroad continue to be relevant. Entry from Canada with the support of Islamist cells there, embarkation from Europe's Visa Waiver Program countries, surreptitious entry from Mexico through human smuggling channels, and recruitment and transportation in the United States are all serious issues for a terrorist mobility strategy. While much attention has been focused on the southern border, the United States' security relationship with Canada is especially important, as suggested by the factors of proximity, less restrictive travel regulations, and scale of terrorist presence there. Similarly, our security relationship with Europe is especially important because of the violent Islamist factions there, as well as scaled back travel regulations. This report, however, does not seek to refine priorities; it assumes a broad vulnerability through all potential points of entry as well as exploitation of our immigration system, and explores a general approach to addressing both.

A strategy to undermine and disrupt terrorist mobility requires that at least eight arenas of action be effectively integrated and continually improved:

- Establishing high standards of knowledge of terrorist mobility;
- Targeting terrorists who act as travel facilitators;
- Aggressively working to shrink and exploit the illicit travel networks (e.g., document providers, human smugglers and traffickers, and other transnational criminals) that are a source of travel facilitation and funds for terrorists;

- Investing in the ability to track individuals *en route*;
- Equipping legal entry and immigration channels to better detect terrorists;
- Denying terrorist access through illegal entry channels;
- Creating a systematic approach to constraining terrorist mobility within the United States; and
- Conducting thorough, post-incident and post-attack terrorist mobility reviews that enable preventive measures to be strengthened and public confidence to be bolstered.

Each element of a terrorist mobility strategy has strong domestic and international dimensions. While the United States has a greater obligation to secure its own entry channels, the job becomes exponentially more difficult—even impossible—without security partnerships with neighbors and allies, greater security within their borders, and greater security of common global travel and trade pathways. This necessitates a greater emphasis on terrorist mobility related diplomacy and leadership in the development of new laws and processes internationally.

Programs and priorities that focus specifically on terrorist mobility are needed to support these elements. Examples include:

- A major, multifaceted, terrorist travel document program;
- Updating the Visa Waiver Program to raise document and identification security standards;
- A multidimensional program targeting terrorist travel facilitators and travel facilitation methods that is analogous to the targeting of terrorist financiers and money launderers;
- Proactive investigative programs at Immigration and Customs Enforcement (ICE) focused on immigration violators who may pose terrorism threats;
- Diplomacy and resource allocation commensurate with the terrorist threats from Canada and Mexico; and
- Requirements for a coherent set of terrorist mobility analytic products, emerging from a periodic all-source assessment produced by the government-wide community involved with mobility.

It is an oversimplification to conceive of the job of preventing terrorist infiltration as a competition between resources allocated to generic

“border security and immigration controls” on the one hand and to “intelligence” about terrorists on the other. The border, transportation, and immigration systems are themselves venues for significant development of knowledge, rules, and processes with which to counter terrorist mobility, for operations against terrorist travel facilitators, and for the application of methods of terrorist detection that go well beyond watchlist use. Development of these measures will strengthen US defenses against terrorists—including through support to offensive operations—and also generally reduce the vulnerability of border and immigration systems.

While there are well established and highly effective programs already focused on terrorist movements, there are some notable weaknesses in our efforts so far. These largely mirror challenges facing the overall counterterrorism effort. Limitations are particularly evident where innovation and nontraditional relationships are called for in and among governmental functions. For example, there is a need for greater infusion of classical intelligence and investigative practices into the border control and immigration systems (analogous to the need to dismantle the “wall” between law enforcement and the intelligence community); for central compilation and analysis of immigration law investigation information; for the law enforcement community to share information with outside analytic units; and for expanded terrorism-related crime control that bridges the United States and foreign arenas. Most importantly, the knowledge and effective activities that do exist must be integrated and deployed for maximum impact. Tactics to gain insight into and disrupt terrorist movements can be optimized only by simultaneous employment of *all* of these operational levers.

Direction, management, and the supporting organizational structures are critical for designing and carrying out such a complex task. Although some key elements are in place, they are not yet sharply defined or authoritatively developed. For example, top officials cannot yet be provided with a baseline report that lists suspected terrorist entries and stays by location, channels, transit paths, and detection and confirmation methods. Only the new National Counterterrorism Center has the potential to ensure the standardized compilation of such basic data, which must come from a range of agencies.

Management elements that must be reinforced in support of a terrorist mobility strategy include:

- The NCTC, which is accountable for strategic direction and for general coordination management, including (under the authority of the Director of National Intelligence) intelligence resources dedicated to terrorist mobility;
- The DHS policy, intelligence, and operational units that provide key strategic input, programmatic and infrastructure designs, and expert intelligence and operational resources;
- The Department of State's leadership and coordination in proposing and implementing a global terrorist mobility diplomacy within the NCTC-designed framework; and
- The Human Smuggling and Trafficking Center (HSTC) as a nascent fusion center for producing global terrorist mobility intelligence and providing operational referrals.

Missing organizational elements include: a management and organization structure for terrorist travel document scrutiny; an organizational framework for investigations by the Federal Bureau of Investigations (FBI), DHS, and State Department of suspected terrorist entries and illegal residence, and a unit dedicated to carrying out transnational investigations of and operations against terrorist travel facilitators; and a systematic structural relationship with State and local officers. A key area of ambiguity is the Department of Defense's role in terrorist mobility countermeasures at US borders, within the United States, and globally.

While there is every reason to move ahead aggressively with the types of improvements this report recommends, we must allow for the possibility that, even in the limited context of terrorist mobility, the post-9/11 organizational changes will not be sufficient to answer the strategic demands made by terrorism. For the foreseeable future, insufficient integration of assets is the most fundamental problem. The structural advantage of having established DHS is that it consolidates agencies with authority in the US border and immigration zone, a legally and geographically distinct arena in which terrorist vulnerabilities can be effectively exploited and our own vulnerabilities reduced. But with respect to terrorist mobility, DHS has an ambiguous and problematic relationship with the FBI, which is the designated but struggling domestic counterterrorism agency.

Also unclear is how DHS will be integrated into a globally networked counterterrorism effort in a structure in which the Department of State leads foreign policy and the NCTC provides strategic direction for counterterrorism.

Terrorist mobility, like terrorist communications or terrorist finance, is an operational concept that is a critical functional component of counterterrorism, as applicable to eco-terrorists as it is to Al Qaeda. As such, it provides a compelling area for practical focus in programs, budgets, and law, which in turn must sharpen and re-shape aspects of diplomacy and politics. Defenses against terrorism continue to be critical. Yet all but the most recent of the national strategies that the government has published since 9/11—the most important of which address national security, homeland security, combating terrorism, and military-related homeland defense—omit mobility as a distinct functional element of terrorism requiring its own operational strategy. A new military strategic plan highlights “movement” for the first time.

National strategies are important because they articulate what we stand for and the risks we face, and provide direction and guidance in acting on those principles and against those dangers. Whatever other issues may be debated concerning current US strategies—and these strategies have evoked a range of responses—there can be no room for debate that countering terrorist mobility deserves to be included in them as a strategic operational element of counterterrorism. This is particularly true since Congress set forth requirements for an initial strategy to constrain terrorist mobility in the Intelligence Reform and Terrorist Prevention Act of 2004.

Addressing the role of terrorist mobility at the highest level of government will make it easier for the priorities and resources for countering terrorist mobility to be tied more closely to our larger terrorism agenda. Thus, it will permit mobility measures to be fully and carefully considered in designing policies and actions to find, punish and disrupt through criminal justice and otherwise, and, if necessary, kill terrorists; to dissuade state sponsors and dismantle safe havens; to keep the most dangerous weapons out of the hands of terrorists; to construct a complete array of homeland security measures at our borders, at critical infrastructure points, and throughout the country; to diminish the forces feeding violent radicalization, and in doing all of these things to build alliances and deepen friendships.

In each discrete area, the United States can make significant progress by making terrorist mobility a more important consideration than it is today. If at the highest level of national strategic and policy discussions, constraining terrorist mobility continues to be casually conflated with maintaining a functional and acceptable immigration system and effective border security—goals that are essential but different and dangerously limiting—we will continue to lose vital opportunities to defend, to deter, and to strike.

INTRODUCTION

Terrorism as a means of war and ultra-criminality is here to stay for the foreseeable future. This is true whether or not states with Moslem populations in the Middle East and South Asia ultimately choose democracy and friendly political and trade relations with the United States. The US military and nuclear forces are too dominant for enemies not to seek alternative means of mounting challenges. And these alternative means can also be accessed by malcontents in our own population. Therefore, identifying and countering the vulnerabilities of terrorist adversaries, stateless or state-sponsored, external and internal, and taking defensive and offensive countermeasures will remain an essential pillar of national security.

The effort to prevent terrorists from attacking successfully requires a systematic and comprehensive approach. All terrorist groups have to execute certain basic operational functions: making decisions, communicating internally and publicly, recruiting and training members, raising and distributing money, and moving people and material. Each of these facets of terrorist functioning offers a potential vulnerability that provides opportunities for designing new offensive and defensive measures. We can create new types of information based on mobility requirements, use them as points of attack, or make them more difficult to carry out—especially secretly.

The US government is already focusing many resources on the spectrum of terrorist operational elements. Efforts are being directed against

terrorist leadership cadres, their communications (including Internet), finance, recruiting and training practices, and their actual and potential sanctuaries. The policy community is particularly engaged in depriving terrorists of access to, and shipping opportunities for, weapons of mass destruction, the ongoing formation and implementation of a terrorist finance strategy, and more recently, updating the legal framework for exploiting communications. One equally important dimension of terrorist operations is mobility—the ability to move people across borders and within nations without being detected by hostile authorities.

Terrorist mobility is a field in which there is significant current activity—the most obvious example being the ongoing strengthening of border screening capabilities. And, the US government is due to provide Congress with a strategy to constrain terrorist mobility. (This is discussed in Section V.) But the subject has received significantly less attention conceptually and programmatically than other dimensions of counterterrorism.¹ This may be in part because it is entwined with the current debate over US immigration policy.

Terrorism by a few and migration by many are twin offspring of modern mobility. Both are outcomes of rapid communications, accessible information, and speedy and expanded transportation—all achievements of the 20th century that promote the global movement of people.² The modern phenomenon of increased mobility combined with the impact of our entrepreneurial economy and immigrant-built society have given rise to a crisis in our immigration policy—one that was emerging in the decade before terrorism became an obvious threat on September 11, 2001. The immigration debate is important in its own right and contentious. With over 10 million residents in the United States in illegal or somehow pending immigration status, and up to 700,000 more people being added yearly, migration would be a critical social and political issue in the United States even without terrorism concerns.

Migration, moreover, like terrorism, is a global reality severely challenging many nations. The nature of the challenges posed by immigration and terrorism are different, however. Immigration pressures may take the form of a refugee emergency or asylum requests precipitated by political violence or social injustice. They are shaped also by political history

and the make-up of existing immigrant communities. But overwhelmingly the forces are economic. The former president of the World Bank, James D. Wolfensohn, summarized the situation this way:

*Over the next 25 years, 50 million people will be added to the population of the rich countries. About one and a half billion people will be added to the poor countries. Many will experience poverty, unemployment, and disillusion with what they will see as an inequitable global system. A growing number will leave their countries to find work. Migration will become a critical issue.*³

Political or economic crises that precipitate sudden large scale upsurges in internal, cross-border, or more distant migration do pose serious issues, including security issues, for migrants and their destination states and these must be taken into account in homeland security planning. But overall, immigration policy turns principally on the answers we give to questions such as:

- What are our economic and demographic requirements and do they require that we take in more or fewer people?
- What limits does national cohesion impose on the ethnic and cultural mix of our populace?
- What humanitarian principles must our immigration system uphold?
- What are the self-evident truths about human dignity and human rights of individuals that immigration policy must preserve?

To answer such questions we must turn to economic analysis and debate, to dialogue among communities and faiths, and to our humanitarian, civil liberties, and human rights commitments. All must be within the framework of the US Constitution. If we fail to find the right balance in answering these questions, we lessen our legitimacy and national unity, thereby weakening ourselves in confronting adversaries.

Terrorist mobility is a subfield of counterterrorism that focuses on constraining the movement of terrorists—those coming to the United States, those already inside the country, and those moving within and between other countries—in order to strengthen our defenses and

offenses against terrorist attacks. Organizations like Al Qaeda use terrorism to conduct low-level warfare to coerce the state, but the acts of especially harmful criminals can also manifest themselves indistinguishably from terrorism. Either way, as political terrorism or crime, terrorist mobility poses very different core questions from immigration policy:

- What travel, immigration and transportation policies can we and our allies establish that will contribute to preventing attacks and to constraining existing terrorist organizations' mobility?
- What must we do to reduce the potential for extended damage to our border functioning if terrorist incursions result in attacks?
- What are the self-evident truths about human dignity, privacy and civil liberties, and the rights of individuals in warfare that counterterrorism policy must preserve?
- What immigration policies would contribute to the broader strategic goal of persuading states and stateless organizations to use diplomacy and political processes instead of terrorist attacks?

Answering these questions effectively will contribute to our offense and defense against terrorism. They will contribute to the prevention of successful attacks that kill people, harm the economy, distort national politics, and sap national strength.

The interface between countering terrorist mobility and immigration policy

The new field of terrorist mobility intersects with the immigration debate in three major ways: in border control design; in management of the level of immigration; and in decisions about whom to admit to the United States as visitors and citizens.

The first is at once old and new—the enhanced tactical significance of border crossings as part of a larger screening architecture. When terrorists need to cross sovereign borders for *any* of their critical functions—communications, fundraising, recruiting, training, decision making, conducting surveillance, and escaping after attacks—their vulnerabilities and our opportunities are greater.

The significance of border crossings for counterterrorism goes beyond the practice of screening to prevent entry by dangerous travelers. In crossing borders (including the legal hurdles crossed virtually at consulates and immigration access points), terrorists *potentially* expose themselves to detection. Whether or not we can intercept them, we must ensure that they leave a footprint. The substantial screening architecture provided by border crossings and associated transportation access points offer the potential for capturing extensive revelatory information critically important to the new national security framework. This in turn adds a new dimension of importance to the personnel and practices dedicated to the border control function and the ongoing budgetary allocation for border infrastructure. It is also an important agenda item for diplomacy and collective agreements. The more effective our screening system and our collective confidence in it, the greater latitude the United States has in deciding how many visitors and immigrants to admit.

The second way terrorist mobility intersects the immigration debate is in the level of immigration and how it is enforced: how many migrants the United States admits legally relative to demand and how effectively those limits are enforced through regulation and criminal laws. The levels set by Congress for immigration are important even if we achieve an optimally effective screening system. When demand for immigration (from employers, newly settled immigrants, and migrants themselves) cannot be met through legal channels, an illegal infrastructure inevitably forms to facilitate the supply. Permeated as the border zone is with human smugglers and fake document suppliers, this is clearly the situation today. The *level* established by law for immigration is important for terrorist mobility because the need for terrorists to remain clandestine can motivate them to interact with the criminal support system for migration. That opportunity should be limited by structural means as much as possible.

But even if the current debate results in a new, more stable balance between demand for entry and ability to meet that demand, some level of human smuggling, travel document manipulation, and remote surreptitious infiltrations will continue indefinitely. The global economic and demographic outlook would seem to portend migration pressures on the United States and other Western and wealthy nations for the foreseeable

future, so that any immigration equilibrium is likely to be imperfect. The more stable and lasting an immigration equilibrium Congress can craft, and the more positive its impact on the rest of the world and their perception of us, the greater will be the US ability to persuade other countries to help suppress and control the global criminal infrastructure for migration.

The third arena in which terrorist mobility intertwines with immigration is in decisionmaking about whom to admit and how immigration is managed, including exclusion criteria and enforcement policy. *Which* visitors and immigrants we admit and how they are treated matters in several ways, apart from the immediate operational impact of effective screening. Successful terrorist organizations collaborate with networks of sympathetic people who can provide willing recruits and supporters. This is a more pressing problem today than earlier in our history, simply because with weapons of mass destruction, individuals can do more damage. Therefore, more attention has to be paid to these rules, with particular sensitivity to maintaining a national consensus about what counterterrorism means are Constitutional and appropriate for a national strategy.

Admission and enforcement policies also significantly contribute to a broader strategic approach that expresses our commitment to individual freedom, open trade, and friendly relationships, and attempts to ratchet down the impetus for terrorism. Visitor and citizenship policies and processes can educate visitors about what is expected of them, and promote immigrants' ability to adapt and thrive, minimizing the possibility of later-arising disaffection or loyalties that turn to terrorism. They can promote positive attitudes toward the United States and seed democratic values, vital skills, and prosperity in other countries. How we regulate and enforce immigration laws and handle terrorism cases is instantly communicated to home communities and affects beliefs about, and ultimately politics toward, the United States. Effective use of the rules can help deter actions to support terrorists abroad. An immigration regime marked by equal respect and fair processes will not prevent us from having enemies, but it will strengthen the perception of legitimacy and help us build global alliances essential to confronting stateless terrorists and criminals.

The new question

The challenge for those making counterterrorism policy is to delineate the portion of border control and immigration policy that deals with mobility for terrorists, and shape it in a way that constrains terrorism and at the same time supports the broader goals at stake in our border and immigration systems.

Following the 9/11 attacks, it was understandable that the public and immigration authorities asked: “What regulatory and enforcement tools for immigration policy should have been and must now be used against terrorism?” Equally understandably, our military, which has not been focused on frontier defense since before the Civil War, is now asking: “What does the military have to offer to border control?” The Department of Defense’s recently published *Homeland Defense and Civil Support Strategy* proposes one possible set of answers.⁴ But these formulations from within the immigration policy field and within the military need to be encompassed in a more direct question, “What practical steps can the United States and its allies take to exploit the terrorist need to be mobile, in order to prevent attacks here and elsewhere?”

Answers to this question should be developed jointly by a variety of experts in consultation with one another, including those in the immigration, national security, and foreign policy communities, and their front line personnel. A community of people with different kinds of knowledge relevant to the problem must participate in the ongoing evolution of a terrorist mobility strategy, just as is occurring in other fields of counterterrorism.

A terrorist mobility strategy

This report seeks to energize the advance of a terrorist mobility strategy (TMS) distinct from, but related to, immigration policy. It discusses:

- Questions that define terrorist mobility;
- The three broad purposes of a TMS;
- Eight arenas of action;
- Direction and management of a TMS; and
- National strategic and statutory frameworks.

Designed as it is to stimulate discussion, this report does not seek to offer a comprehensive account of what we know about terrorist mobility and what we are currently doing. As discussed in Section V, Congress in the Intelligence Reform and Terrorist Prevention Act of 2004 charged the National Counterterrorism Center (NCTC) and the Human Smuggling and Trafficking Center (HSTC) with producing reports and designing strategies that will both describe terrorist travel and report on the implementation of programs to constrain it.⁵ This report considers aspects of what is known about terrorist practices but focuses primarily on what we need to find out. It suggests what we ought to consider doing and comments on current initiatives such as immigration-related policies and programs, all from the perspective of a coherent terrorist mobility strategy. It draws on a variety of sources, including work performed by the 9/11 Commission, discussions with government officials, government reports, academic and policy papers, and writings about strategy, terrorism, terrorist groups, and immigration and crime control.

Pervasive issues

Three pervasive issues emerge in considering the predicates for a terrorist mobility strategy.

The first is the need for setting higher knowledge standards at every stage of our border and immigration system. A current bromide is that “intelligence” is not the solution to border security because terrorists have too many gateways available to them, so we must focus instead on across-the-board immigration “enforcement.” This is both true and false. A devastating terrorist plot may involve only a handful of people from almost anywhere in the world. This places a premium on marshalling knowledge of all kinds to anticipate the emergence of terrorist groups and to track terrorists once they emerge. But we cannot rely entirely on classic standard intelligence developed by the intelligence community and fed into our border and transportation systems. Instead we must build a new array of terrorist mobility information methods and sources, combining intelligence collected by the intelligence community with intelligence and information, including about terrorists, developed and applied by officials within the border and immigration community. To be able to adjust the immigration system as needed, a dynamic and

comprehensive system is mandatory, one that integrates information and continually uses it to improve offensive and defensive measures.

We are still excluding, losing, or wasting information absolutely critical to understanding the routes and methods of terrorist movements developed in immigration adjudications, databases, and law enforcement investigations. This information ought to be retained and electronically accessible in border control information systems and in investigative files. Law enforcement investigations should be treated as sources for information leading to new countermeasures, as well as a basis for prosecutions. Some level of centralized integration and analysis, with effective communication to the front lines and policymakers are at least equally important—and lacking.

Second, terrorist mobility cannot become a distinct and powerful focus for counterterrorism without developing new arrangements for its direction and management within the larger counterterrorism effort. A great deal of attention has been given since 9/11 to the “wall” dividing the intelligence and law enforcement communities, and to the foreign-domestic divide in counterterrorism. Comparably deep and damaging disjunctures persist between the border and immigration community and the intelligence and law enforcement communities, and the military. Over four years after the 9/11 attacks, information-sharing difficulties still exist, sometimes willfully due to organizational competition, sometimes as a result of organizational cultural differences that still exist between law enforcement and intelligence agencies, and also because of a failure to significantly close the information-sharing gap between federal, state, and local governments.

The border and immigration sphere is legally and practically distinct, and must be supported by intelligence, law enforcement, and military organizations, which must also participate in coordinated exploitation of its operational and tactical resources. Establishing new types of structures and arrangements for working together while transforming the work that is being done is a difficult and long-term challenge.

The third issue is the need to integrate terrorist mobility into the larger agenda of cooperative law and lawmaking surrounding terrorism.

Mobility issues generally must be given more prominence as an element of diplomacy and foreign assistance, especially in order to work with security partners to bring historically secret capabilities into legal and shared frameworks. This is what it will take to make breakthroughs on sharing watchlists, among other complementary counterterrorism resources. And not all problems are shrouded in sovereign security-related secrecy. The full panoply of travel and immigration system law—from birth certificate to passport issuance, inspection regimes, and travel agency regulation, to criminal laws governing travel document forgery and human smuggling—is ripe for the same type of heightened bilateral, regional, and multilateral attention devoted to the security of international financial flows.

Our immigration laws are fundamental to our character as a people, the functioning of our economy, the make-up of our society, and our integrity as a democracy rooted in law-making. But we have also entered an age when nuclear, biological, and chemical weapons are potentially accessible to terrorists, and terror is already being sown. While resolving conflicts about immigration policy, and ensuring the political and financial resources to construct and maintain travel and trade channels vital to our economy, we must also sharpen and deepen efforts to constrain terrorist mobility. Policies and mechanisms in the counterterrorism and immigration arenas should be mutually supportive but they are not necessarily the same.

Our approach has to combine effective counterterrorism, specially designed and infused into all layers of our border and immigration regimes, with an orderly immigration system that promotes prosperity and welcomes peaceful people. This approach will not spare us from difficult decisions about executive power, privacy and civil liberties, how to draw lines against violence-inducing speech, the law governing terrorist detainees, or when to share secrets and technology with allies.⁶ A terrorist mobility strategy will not prevent illegal migration. But it will yield something vital—more tailored and effective measures against terrorists—and also contribute to a safer, more orderly immigration system.

I. DEFINING TERRORIST MOBILITY

“Intelligence” as a cornerstone of counterterrorism and homeland security strategy since 9/11 has been limited in two ways that have been problematic for maximizing our effectiveness against terrorists. First, priority has been given to subjects for collection and analysis that were well established in the intelligence and national security community prior to 9/11 as relevant to counterterrorism—leadership cadres, terrorist finance, and communications, for example. Second, the “intelligence” needed to inform counterterrorism and protective measures has been conceived of as deriving primarily from classic intelligence methods and operatives, and not criminal investigations, immigration adjudications, and border crossing data.

To exploit terrorists’ needs to be mobile and cross borders, we need to significantly revise both of these understandings. Terrorist mobility must be added as a top tier matter for attention in counterterrorism. And the concept of terrorist mobility intelligence must be broadened to become terrorist mobility knowledge. (Terrorist mobility knowledge is discussed in Section IIIA.)

Enemy movement has a long history as a topic of study in military science. When the Soviet Union’s armed forces were the United States’ central security concern, the field studied such elements as logistics, transportation capabilities, the significance of movements in and out of barracks, training exercises, likely attack routes, and deployments that might signify land, sea, and air attacks. Enemy movement, with the exception of espionage, was defined largely by how conventional armed forces moved.

Today’s newly critical terrorist threats come from smaller organizations and individuals. Like Al Qaeda operatives, they may be part of larger political movements. They may include clandestine agents of states. They may be home-grown violent malcontents or ideologues. They may be violent supporters of global causes or criminals akin to terrorists in the scale of their activities. They can mingle in the populace, travel

singly and in twosomes, and they do not wear government-issued uniforms or insignia of military forces.

Because these types of adversaries and security threats move around in different ways from conventional armed forces, a new chapter in the study of adversary mobility must be opened. The more specifically we are able to describe terrorist travel and transportation practices, the greater potential we have to take advantage of offensive and defensive opportunities: to invent new tools, plug holes, fortify systems, adapt legal frameworks, and institute measures of deterrence.

Broadly defined, terrorist mobility encompasses all facets of terrorist movements. As a foundation for action, we must find out what simplifies terrorists' travel and what makes terrorists and other criminal clandestine travelers vulnerable to detection. The following seven subject areas mark out the defining elements of terrorist mobility:

Management of the travel function. We routinely study how armies, navies, and air forces organize logistics and carry out their movements. Who plans and arranges for travel and transportation in terrorist organizations? What functions are central and which are a local responsibility? Who are the travel facilitators? Are they internal or external? These questions require answers generally and by terrorist organization.

International geographic routes and transportation practices.

What geographic destinations (frequency of direct nation to nation travel and via other nations), and transportation routes (air, sea, land) and modes (airline, ships and boats, busses and trains) are used? Where are the key jumping off points and chokepoints? Which carriers are preferred, and what are the means of purchasing passage? Do the groups train in particular kinds of transportation, e.g. small boats or airplanes?

Illegal entry and residence tactics. A baseline catalogue kept up-to-date with terrorist illegal entry and residence or embedding tactics is an essential foundation for a terrorist mobility strategy. Entry into the United States through illegal channels has received most of the public attention because of the large numbers of migrants attempting entry across the Southwest border. But the steps terrorists

take to facilitate residence in a particular area for short- or long-term duration, depending on their needs, are equally important. Some length of time is needed for fundraising, recruiting, planning and execution. Without basic information about entry and embedding tactics, government officials cannot systematically examine what might be done to mitigate or eliminate the vulnerabilities that terrorists are exploiting.

Entry Through Legal and Illegal Channels

“Cleanly” and “legally” were the terms that senior intelligence and law enforcement officials used to describe Al Qaeda operatives’ entry into the country to carry out the 9/11 attacks. This terminology is seriously misleading and has led to a gross underestimating of the central role and capability of border zone officials in countering terrorist mobility. Since the hijackers definitely did not enter the country “legally,” and most of them not “cleanly” either, we must find a more accurate set of terms to describe terrorist tactics for entry and residence.

Defeating the border and immigration controls of sovereign states is comprised of two basic approaches. The first is to make *illegal use of legal channels*. The second is to use *illegal channels*.

Legal channels used illegally includes any kind of undercover travel and residence that passes through any of the legal checkpoints nations have established to manage their borders or frontiers and their immigration systems. Examples of entry include a terrorist obtaining a tourist visa from a consulate or passing through an air port of entry as a tourist from a Visa Waiver Program country. Examples of residence or embedding include fraudulent exploitation of the rules for marriage and asylum, as well as refugee, student or religious worker status. If a legitimate visitor, lawful permanent resident, or naturalized citizen is recruited by a terrorist group, once he or she becomes a terrorist, attempting to cross borders or maintain his or her immigration status is using legal channels illegally.

Use of *illegal channels* consists of any kind of stealth travel entirely outside immigration controls and border ports of entry. Surreptitious entry into the United States by boat or land crossings over remote places along the Mexican or Canadian borders; mountain crossings into

Afghanistan from Pakistan; ferry crossings from the horn of Africa into the Arab peninsula; and land border crossings from Syria into Iraq are examples. An Islamist terrorist group's use of human smuggling routes through Mexico also would be a use of illegal channels.

This framework allows a more precise description of the mobility tactics Al Qaeda used to carry out the 9/11 attacks. They made *illegal use of legal channels* to enter and remain in the United States for the 9/11 attacks. Their method was to deceive border authorities (consular, immigration, and customs officers) first, as to their personas as individuals with bona-fide identities and travel purposes, and second, in most cases, as to the integrity of their supporting documentation. (They were also able to evade the intelligence community and escape the notice of domestic law enforcement.) Only after the fact did immigration authorities learn of these operatives' Al Qaeda affiliations, and the 9/11 Commission stated that fifteen of nineteen hijackers had presented travel documents with terrorist indicators potentially detectable by knowledgeable authorities.⁷

A well known example of deceptive presentation of personas and purposes may be helpful in clarifying how the 9/11 conspirators entered illegally using legal channels. The Department of Justice's Office of Special Investigations has had a program since 1979 to identify, investigate and take legal action against former participants in Nazi persecution who reside in the United States. These individuals had passports and visas that passed inspection and they became US citizens through official procedures. For many years they lived in communities as if they were here legally, and were deemed to be so by government authorities. As with the 9/11 Al Qaeda operatives, no one probed the Nazis' personas—their histories, their motivations—at the time they were admitted. However, the US government later determined that these official decisions had been erroneous—these persecutors had entered and been admitted, and became naturalized citizens under false pretenses.

Like these Nazis, any Al Qaeda or other terrorist operative is entering the United States under false pretenses—presenting a false persona—to defeat the US bar to their entry. Terrorists may also take deception one step further and construct entirely new identities and histories, as do spies or other foreign agents. The construction and presentation of

false personas is therefore an important and challenging aspect of terrorist mobility.

As with most of the hijackers, terrorists may use travel or supporting documentation with fraudulent or revealing elements as a deception tactic. Even if documentation is not itself entirely false or illegal, there may be other indicators of deception. The indicators—on travel documents, on someone’s person, or in their demeanor—may be in themselves legal or illegal. A terrorist passport may show a suspect but not illegal travel pattern, or include a genuine travel stamp associated with a corrupt inspector. In the illegal range, a terrorist may have violated other nations’ laws by acquiring a passport issued by a nation of which he or she is not a citizen or by having an expired visa. An individual may be wearing certain clothing or jewelry or a tattoo that is not prohibited, but which would suggest to a knowledgeable official that the person may be a member of a violent gang.

The danger in describing the 9/11 hijackers’ entry as “clean” and “legal” lies in the implicit assumption that border zone countermeasures can be so easily defeated that, for strategic operational counterterrorism purposes, they should be discounted relative to reliance on a combination of classic foreign intelligence and military methods abroad, law enforcement and intelligence at home, and exploitation of well recognized vulnerabilities like finance and communications. This attitude persists in national strategy and policy circles today. But it is misguided. Countering terrorist mobility methods, including through systematic, comprehensive measures in legal entry and residence channels, provides a necessary and powerful set of tools for homeland security and global counterterrorism.

Methods of using legal channels illegally by geographic region.

According to Spanish newspapers, when authorities detained the chief of Al Qaeda in Southeast Asia and organizer of the Bali bombing, Riduan al Isomuddin (known as Hambali), he had in his possession the passports of two Barcelonans whose photographs he had substituted with his own.⁸ One of the 9/11 hijackers, Ramzi bin Alshib traveled throughout Spain and used the passport and credit card of an American doctor who had been robbed in Barcelona. Cumulative study of terrorist mobility would analyze patterns and practices in the use of travel documents

among other tactics associated with using legal channels illegally. What nations are quarries for travel documents? When do terrorist organizations use particular nations' documents?

Methods of using illegal channels by geographic region. Detailed mapping of illegal entry routes (land, sea, and air) is a long-term challenge for the study of terrorist mobility. The Mexican and Canadian borders of the United States, and the Iraq borders are examples of where there is a need for a high level of detailed planning. In the case of Iraq, a typical foreign fighter might begin a journey into Iraq with exploitation of the legal entry system by obtaining travel documents through official channels to enter Jordan, Iran, or Saudi Arabia, and then use illegal entry channels to cross into Iraq between governmentally staffed border entry points.

Terrorist interactions with the illicit travel infrastructure.

Terrorists using *either* type of entry channel—*legal or illegal*—may seek different degrees of support from criminals and criminal networks that operate independently of terrorist networks. These range from no reliance at all to obtaining the services and/or support of corrupt passport and border officials; document theft rings, procurers, and forgers; human smugglers and traffickers; or travel agents. Support from intelligence and military services may be a factor, e.g., the support provided by members of Iranian intelligence to Al Qaeda operatives in concealing their transiting of that country. Describing the illicit travel infrastructure and how a terrorist organization is using it, as well as describing it as a market with services available at particular prices, can define the scope of terrorist mobility and help define goals for a terrorist mobility strategy.

The legal and cultural framework for immigration and citizenship. The legal framework for border crossing focuses on the methods of deceiving border officials and their supporting technology to enter a state illegally. The legal framework for immigration and citizenship would focus on the policies and procedures for issuing passports and other immigration benefits. Does a state virtually give away citizenship, the way states may create banking havens? Does it offer sanctuary to groups proscribed elsewhere? What are the controls on passport issuance? How secure are arrangements for work visas? Which states have biometric passports and how are biometric records safeguarded?

What states have national identification cards? How corruptible are border-related authorities?

The cultural framework for immigration and citizenship would address sociological questions about migration and integration, which are related to terrorist mobility as well as other aspects of terrorism. Relevant questions today concern the overall environment for local recruiting of Islamist terrorists in the United States and the impact of Islamist movements in Europe on US security. Such studies would support ongoing assessment of whether effective measures in the border system are leading to attempts at local recruitment, and to inform residence, naturalization, and border process policies.⁹

These seven categories of information and intelligence, which illustrate the type and range of knowledge that describes terrorist mobility, are analogous to military science's comprehensive descriptions of the elements of armed forces' mobility capabilities. Terrorists' need to be mobile provides us with an opportunity to develop an operational strategy to exploit that vulnerability.

II. PURPOSES OF A TERRORIST MOBILITY STRATEGY

A US and global terrorist mobility strategy has three purposes:

- Defensive—to secure travel, immigration, and transportation channels, at US borders and globally, from undetected terrorist movement and from attack;
- Offensive—to exploit vulnerabilities exposed by terrorists' need for clandestine transnational and internal movement in order to disrupt these individuals and groups; and
- Deterrent—to raise the risk of movement using defensive and offensive measures, so that it becomes a factor in deciding whether to attempt attacks.

These goals are analogous to those of domestic and global financial counterterrorism. Financial institution laws and regulations are designed to defend the global financial system from easy terrorist and criminal access and disruption; banking transactions are employed offensively through interceptions that reveal trails from visible financiers to elusive terrorists; and constraining terrorist finance is a worldwide goal, aiming to reduce the financial network accessible by terrorists, diminish terrorist access to funds, raise costs, and impede operations.

A set of methods aimed at constraining movements, therefore, must aim to impede terrorist organizations and make operations more costly, dangerous, and uncertain, and thwart or stop as many attacks as possible. The potential for major impact is not only in contributing to the disruption of particular operations. If a terrorist mobility strategy sufficiently impedes transnational terrorist movement and entry into the United States, terrorists will have an incentive to develop local recruits and minimize the number of inserted agents. This reshapes the field of engagement in our favor, because it is easier to take preventive measures in our own country than in other countries.

Even an effective terrorist mobility strategy, however, cannot by itself be a decisive factor in causing terrorist organizations to cease seeking to attack, much less to change their political program. We ought to be able to significantly reduce risks of undetected entry into the United States, but eliminating the risk that terrorists will find a way to enter and to reside here is not practical or possible. Consequently homeland security strategy also calls for special efforts to reduce vulnerabilities in critical infrastructure facilities and sectors whose destruction could cause major damage, for priority measures against catastrophic threats like bio-terrorism, and for investment in emergency preparedness and response to enable us to recover rapidly from attacks that may occur.¹⁰ Moreover, like terrorist finance or any other single operational element, exploitation of terrorist mobility is only one aspect of an integrated operational strategy that encompasses communications, sanctuaries, and other elements. Even this larger integrated effort is unlikely ever to provide an *absolute* deterrent to terrorism. Operational counterterrorism methods are one dimension of a larger strategic approach that is political, engages in diplomatic dialogue and ideas, and joins other states in collective lawmaking.

Among functional elements, however, the magnitude of the role of mobility-related techniques in counterterrorism would seem to be at least as significant as funding-related techniques. Watchlist hits are one example; legal action against suspected terrorists is another. A recent sample of one hundred terrorism defendants shows that 80 percent were charged either with immigration fraud or with identification fraud, a category that included forgery or false use of passport; misuse of a passport; fraud and misuse of visas, permits, and other documents, as well as fraud in connection with identification documents and Social Security fraud.¹¹ Although there is reason to doubt the strength of some of the underlying terrorism claims, which cannot be demonstrated through mere statistics, the point here is that the vulnerability to interception and the legal jeopardy created by the need to travel to and circulate within the United States clandestinely is significant.¹²

In practice, the three purposes of a terrorist mobility strategy overlap and require cooperation, coordination, and reconciliation for their optimization. Detection at border crossings is clearly essential for defensive purposes, but it is equally critical as an element of offensive tracking of individual terrorists to discover and disrupt operations; the ability to monitor border crossings also makes possible longer term analysis that leads to new legislation, regulation, and reengineering of border control processes.

This overlap among defensive ends, offensive tactics, and methods of deterrence necessarily leads to as great a need for security alliances as for homeland-based security measures. A key to our terrorist mobility strategy must be working cooperatively with foreign governments by sharing critical information, assisting on the deployment of information technology systems at key border crossings around the world, and assisting in the design and issuance of secure travel documents.

Cultivating and marshalling all the intelligence, information, and operational resources relevant to these tasks presents a new and formidable challenge for government action, organization, and leadership. The first step is to define the procedural and operational elements of a terrorist mobility strategy.

III. ELEMENTS OF A TERRORIST MOBILITY STRATEGY

A basic set of deterrent, offensive, and defensive countermeasures can be set forth based on what is known about the threat today, on our experience so far, and on following the logic of a focus on mobility. To list them here is to present these measures—not necessarily altogether new—within a single terrorist mobility framework. The advantage of a single framework is that it enables counterterrorism leaders to decide how to allocate resources among them, and to shift those resources according to the threat and state of US and security partner capabilities. The following eight elements deserve emphasis.

- A. Foundation: Terrorist Mobility Knowledge
- B. Targeting: Terrorists Who Act as Travel Facilitators
- C. Crime Control: Attacking Illicit Travel Networks
- D. Global Awareness: Tracking Terrorists *En Route*
- E. Border and Immigration Management: Securing Legal Entry Channels
- F. Perimeter Control: Denying Access Through Illegal Channels
- G. Domestic Security: Constraining Terrorist Mobility in the United States
- H. Recovery: Post-attack Terrorist Mobility Reviews

Omitted from this agenda is a separate foreign relations element, focused on securing global travel through coordination, law, and diplomacy. The relevance of foreign states in constraining terrorist movements cannot be overemphasized, and prominent and active pursuit of terrorist mobility-related agreements with security partners near and far is integral to each of these elements. This report refers throughout to the pervasiveness of the need for foreign partnerships in countering terrorist mobility. Mobility issues inevitably must take a more prominent place in our foreign relations and diplomatic agenda, as they already have, notably with Canada, Mexico, and Europe.¹³ Although the lead role of the Department of State is clear, managing a terrorist mobility strategy across the domestic-foreign divide raises difficult issues of direction, management, and organization. These are discussed in Section IV.

A. Foundation: Terrorist Mobility Knowledge

Raising the information level about terrorist mobility, in contrast to terrorist finance, is not yet generally recognized as a distinct, priority need among policymakers. Terrorism specialists who may know the names of terrorist leadership and major terrorist financiers are unlikely to know the names of major terrorist travel facilitators. Immigration policy specialists who know the level of immigration to the United States by ethnic group and decade are unlikely to have access to the overall number of terrorist suspects denied entry to the United States since 9/11 and at what locations they were detected. And developing an “information culture” or “knowledge culture” does not have the same visibility as attempting to block access across the Southwest border with patrols and fences. Yet detailed knowledge of terrorist movements is essential to acting against and assessing the ongoing risk of hostile entry and residence posed by Islamist terrorists in Canada, Europe, and elsewhere.

We need to address the two main causes for the current lack of information about and strategy to contain terrorist mobility. One cause is historical—the relative lack of attention at the highest levels of our national security community to terrorist mobility as a subject of strategy, planning, intelligence, and operations. To change this, we must revise national strategy, which is discussed in Section V.

An equally important and far more pervasive obstacle to an effective strategy to constrain terrorist mobility is a narrow view of the types of knowledge and the methods of knowledge-gathering required to develop and execute offensive and defensive actions. “Intelligence” is the limited label we have inherited to describe capabilities at the core of counterterrorism, and it is understood in its classic sense of being largely foreign-based and carried out by intelligence services supported by technical means. Because it is primarily foreign-based and to a lesser extent trained on domestic targets, a view has emerged that “intelligence” is not concerned with safeguarding the operation of our immigration laws and processes, for which “enforcement” is required.

To equip ourselves to counter terrorist mobility, we must revise the dominant view paradigm, reinforced by our *National Strategy for Homeland*

Security, that “intelligence and warning” supply the necessary terrorism-related knowledge, which in turn supports “border and transportation security” and plays a new and larger role in “domestic counterterrorism”; that these three functions are largely carried out by separate authorities in separate realms, with the wall between the foreign and domestic intelligence players being dismantled; and that immigration system improvements are not otherwise implicated.

Updating the model for terrorist mobility knowledge requires first and foremost that we be clear about what we want to achieve by using that knowledge. The goal is to exploit the vulnerability that arises from terrorists’ need to be mobile—but adopting this offensive goal will enable us to design and build border and transportation systems (including personnel structures) that are far better equipped to intercept, prevent, and deter terrorist exploitation.

Knowledge to exploit offensively and defensively terrorists’ movements or their other operational needs is not a focus of current homeland security strategy. The *National Strategy for Homeland Security* recognizes four primary types of knowledge. Two of these are “tactical threat analysis,” and “strategic analysis of the enemy.” Knowledge relevant to disrupting an unfolding plot—like the identification of a terrorist indicator on a passport—is an example of “tactical threat analysis.” Knowledge of a terrorist organization’s transit methods contributes to a deeper understanding of terrorist organizations’ capabilities, and thus is an example of “strategic analysis of the enemy.”

While terrorist mobility intelligence and information contribute to each of these two types of knowledge, that is not all they do. Tactical threat analysis is relatively immediate and plot-focused, while strategic understanding is longer term, and looks at the political and social forces driving terrorism. Like measures against terrorist finance, countering terrorist mobility is better understood as occupying an intermediate realm, “operational strategy,” which looks at a whole set of methods systematically, targets them offensively, and improves our own defenses against them. Intercepting a terrorist at a port of entry is *tactical*; improving the necessary architecture to screen for terrorists is *operational*; understanding the social and political make-up of Muslim immi-

grant communities supplies essential *strategic* understanding. Although terrorist mobility is essentially an operational category, it encompasses all three types of knowledge.

Two other forms of knowledge identified in the initial *National Strategy for Homeland Security* are related to vulnerability to terrorism. Both of these—first, assessments of the likely consequences for the American people of terrorist attacks on particular facilities and sectors, and second, the mapping of actual terrorist threats and capabilities against those vulnerabilities in order to set priorities for risk management—are also relevant to a terrorist mobility strategy. Travel and transportation are key sectors where reducing vulnerabilities and strengthening defenses are critical. However, preventing terrorist *attacks* by terrorists against our “border and immigration system” as primary targets is not so much at issue here, as is terrorist *exploitation* of our border and immigration systems as a step toward an attack. Terrorists cannot seek to blow up our immigration system in the same way they might seek to blow up an LNG tanker in a port (although cyber security is as relevant to immigration as to other government functions). We reduce vulnerability in the border and immigration sectors primarily to prevent death-dealing attacks on facilities, mostly although not exclusively in other sectors, that, in addition to causing death and destruction, would have negative ripple effects on travel and transportation, as happened after 9/11.

Fundamental deficits exist in the knowledge available to policymakers and to front-line officials that is needed to support an operational strategy of countering terrorist mobility. For example, surely a basic requirement is a report for top officials and front-line managers that informs them of the total number of suspected terrorists attempting entry from all locations, and identifies terrorist and detection methods. Producing this baseline is in fact relatively complicated, due to the many agencies that must cooperate in providing information and the careful analysis it requires. But without it, how do officials monitor and assess objectively the relative risks at the Southwest or northern borders, or among air, land, or maritime entries? Basic factual information must be considered together with more strategic assessments—for example, the number of adherents of violent Islamist ideology in Canada and Europe and the

size of the populations vulnerable to such thinking, as well as the likely embarkation nations for self-starter terrorists (like Ressam) and for terrorists involved in more catastrophic plots. And to choose which of the many vulnerabilities in our own systems require immediate attention, we need to develop intelligence about specific operational threats, as occurred in the case of closing the “Transit Without Visa” program.

As with other aspects of counterterrorism, developing effective terrorist mobility countermeasures requires that new and even higher standards of knowledge requirements be adopted by front-line organizations. *Some* information and analysis is needed to anticipate the level of economic migration and to actually find migrants approaching from Mexico or overstaying visas from South Asia; *more* information and analysis is needed to interdict and deter human smuggling and other transnational criminal organizations and actors. It is not enough that we obtain the data, as we already do in many cases; extra steps must be taken to organize it in a way helpful to countering terrorist mobility.

Four existing models for developing information about transnational movements are important sources for a new framework for developing knowledge essential to a terrorist mobility strategy. Each source has something to contribute and limitations.

- The military study of armed forces’ movements and border defenses provides the most apt analogy. As in conventional open warfare, counterterrorism operations must scrutinize the movements and potential trails of people and materials as a means of attacking havens and intercepting movements. A limiting factor is that armed forces’ movements are too different from individual and small group practices to provide an exact template. Moreover, most of the key authorities and resources for acquiring relevant information are held by civilian border authorities, not the Department of Defense.
- Counterespionage and espionage provide a model for developing information about clandestine entry and exit from countries. The relevance of historical infiltration and exfiltration practices is limited because espionage and counterespionage have been directed largely

at government intelligence services; terrorist organizations draw on a wider range of travel facilitation sources than governments.

- Accurate migration information is important because it describes the larger flows in which criminals are active and terrorists may be concealed. Immigration and migration flows turn on economic, political, and sociological factors that provide one relevant context for terrorist movements; however, they shed no light on how terrorist organizations make and carry out decisions to travel.
- Information derived from transnational criminal investigations and from immigration, customs, Coast Guard, and Border Patrol inspections and investigations is highly relevant to mobility-related counterterrorism operations. Methods used by criminals and immigration and customs law violators overlap those used by terrorists. Unfortunately, many civil and criminal law regulatory and enforcement agencies lack well developed information management practices to centrally collect, analyze, and disseminate knowledge of travel tactics developed in audits, adjudications, inspections, or criminal cases.

A new field of terrorist mobility knowledge is required in which the sum is more than the parts inherited from these important historical approaches. The new field needs to constitute a single whole, whose functions are broadly overseen centrally but carried out by multiple entities. There are six basic challenges:

- Integrating collection requirements and procedures for terrorist-specific mobility information;
- Managing—including sharing—terrorism-specific and related general mobility information;
- Generating knowledge about terrorist mobility tactics through information analysis;
- Communicating terrorist mobility knowledge to the front lines and policymakers;
- Integrating terrorist mobility knowledge with policy and operations; and
- Knowing what is working to inform improvements.

Because we are still hobbled by a limited view of the role of knowledge in intercepting terrorists—including the idea that “intelligence” and immigration enforcement information lie on two sides of a policy divide—it is worth discussing something of what is involved in each of these six information arenas, each of which is essential to countering terrorist mobility. The categories are abstract in comparison to discussions of the terrorist watchlist or operational programs, but their application is essential to effective counterterrorism.¹⁴

1. Integrating collection requirements and procedures for terrorist-specific mobility information

The first challenge is simply obtaining hard-to-acquire information about terrorist movements, transportation, and travel practices. This includes information such as a particular terrorist organization’s preferred routes between countries or its passport practices by country.

Intelligence officers, front-line border officials, law enforcement investigators, and the military all acquire information relating to entry to the United States. The word “collectors” historically has denoted intelligence agents, who would encounter the enemy national target in the first instance—a CIA case officer encountering a source in Berlin or Moscow. But information collection relating to terrorist mobility potentially takes place in a wide range of different and unexceptional “spaces,” many of which historically have not been typically associated with significant intelligence collection against individuals: overseas in friendly countries; on the high seas; at US borders, including visa offices, coastal waters, and land borders, as well as air, land, and sea ports of entry; and within the United States. These involve a plethora of novel collection opportunities and governing laws. So in the terrorist mobility context, as a practical matter, key collectors include *anyone who may encounter a terrorist in the first instance* in the normal course of their duties. This includes, but is by no means limited to, intelligence agents active in or outside the United States who derive terrorist mobility intelligence from such sources as computers or interrogations of detainees. Important collectors include border officials who adjudicate visa applications and inspect visitors, law enforcement officials who stop or arrest individuals and in the course of doing so obtain documents and information, and travel and transportation sector employees who make reservations and deal with travelers.

A policy decision to treat terrorist mobility as a separate dimension of counterterrorism should be made as a step toward strategic operational management of collection requirements. As with other fields of counterterrorism, terrorist mobility collection requirements must include intelligence sources, domestic and international law enforcement sources, diplomatic sources, and publicly available sources.

2. Managing—including sharing—terrorism-specific and related general mobility information

Various components of the US government have embarked on increased information management potentially relevant to terrorist travel. Maturing of border information systems began with the Customs Service modernization program in the mid-1990s, a long-delayed effort to enable the Customs Service (now absorbed into DHS' Bureau of Customs and Border Protection) to process goods and collect revenues more efficiently and effectively using upgraded computers and reengineered processes. Systems relevant to terrorist mobility strategy include those that provide terrorism-specific information and systems that relate to border crossing or immigration management generally. These are managed, accessed, and shared in varying degrees of adequacy.

Terrorism-specific information. A core portion of terrorist mobility information depends on the intelligence community. The main information pillar is the all-source database of data about individual terrorists maintained by the National Counterterrorism Center, which downloads certain information to the Terrorist Screening Center (TSC), which maintains a Terrorist Screening Database (TSDB) that contains US person and non-US person information. The TSC is accessed by border and law enforcement agencies and is presently funded under the FBI budget. Although there is progress to be made, this dual-centered architecture provides a very workable arrangement for developing and sharing information relevant to terrorist mobility.

A new challenge is to create an equally workable arrangement for collecting and managing access to *terrorist travel document-related information*. Elements of a solution include:

- A central physical collection of *terrorist* travel and supporting identification documents;
- A comprehensive electronic library of digital images of complete *terrorist* travel and supporting identification documents;
- A definitive, continuously updated electronic reference library of exemplars of *legitimate* travel documents and supporting identification documents from all nations;
- A comprehensive database of United States and international *lost and stolen passports and visas*;
- A comprehensive electronic library of digital images of complete *criminally developed* travel documents and supporting identification, emphasizing those produced by criminal sources and organizations most likely to be tapped by terrorist groups—criminal travel facilitators, human traffickers and smugglers, arms smugglers, and narco-traffickers.

Aspects of these collections are underway. An electronic library of legitimate travel documents has been launched by several nations with participation by DHS' Forensic Document Laboratory (FDL). A complete, continuously updated electronic collection is needed in order to establish a computerized document-checking system in front-line border computers. (The organization of a terrorist travel document capability is discussed in Part IV.)

Sharing of terrorist mobility information remains a significant problem. Horizontal information-sharing does not occur automatically among institutions. The costs and problems associated with information-sharing require that there first be a formal process to assess collection needs and systems for accessing mobility information.

A notable limitation at present is the lack of access by other agencies to information about terrorist travel contained in investigative files of FBI or Joint Terrorism Task Force counterterrorism and immigration cases. Valuable information on how these people entered the country exists in these files, but may not be systematically gleaned for patterns of entry. It is not generally accessible electronically, and there is no systematic practice for otherwise extracting and sharing it, so it is generally unavailable for all-source analysis. This lack of information-sharing of terrorist travel

information is a significant, immediate barrier to achieving a higher level of effectiveness in denying terrorist access to the United States. It may or may not be a problem for “connecting the dots” in order to supply warning of imminent threats. But it certainly prevents the information from being assembled into a larger whole, which would have much greater significance for policymakers and for front-line officers and their supervisors.

This is not surprising since data analysis has been a little-used tool in investigating and referring cases for prosecution. The focus of law enforcement has expanded from post-incident investigation to warning of and preventing possible terrorist activity. But this mission expansion has not resulted in a commensurate growth in the use of nonoperational analysis and partnerships with those entities that could provide it. Absent such a comprehensive picture of terrorist mobility, front-line border officials make decisions based on what they know about violations of the immigration system, which are overwhelmingly unrelated to terrorism. While some tactics may be the same or similar, some will certainly be unique. All of them need to be considered.

The heavily classified-source information concerning terrorists and terrorist travel documents represents the most manageable part of the overall picture of terrorist mobility-related information management.

General traveler information. A major challenge is ensuring that watchlisted individuals are detected and that previously unknown terrorists are identifiable when they undertake entry or later immigration processes. To allow border officials to make optimum use of the name-based watchlist, we are investing in major new border information systems to expand the capabilities connected with background checks at various points of the travel, transportation, and immigration systems. Even a partial list of the information agendas of the US border and immigration control system and the transportation system shows the breadth and complexity of the transformation being undertaken:

- The student tracking system (SEVIS);
- The biometric entry-exit system (US-VISIT);
- Other biometric screening systems instituted by various departments, agencies, and divisions of agencies;

- The airline passenger data transmission system;
- The Automated Targeting System for screening incoming passenger data;
- Multiple registered traveler lists with incompatible data formats;
- Expansion and revision of the US passport and/or a North American identification document;
- Multiple credentialing systems for transportation mode and critical infrastructure access;
- Standard-setting for the states' driver's license systems;
- Standard-setting for the states' birth certificate systems; and
- A proposed electronic employee immigration status verification system, included in the major pending immigration reform bills.

And this list does not include improvements to the Social Security system, changes to the visa and naturalization processes, any classified systems, an automated targeting system for exit screening, or access to a database in which citizen birth and death information can be verified.

Understanding how these various but functionally overlapping systems contribute to countering terrorist mobility—in comparison with their use in managing immigration—as well as sticking to the resulting priority agenda for their development and allowing systems time to mature, be revised, and become reliable, are central challenges for a terrorist mobility strategy.

With terrorist finance programs, much investigative work occurs in systems owned by the private sector, and specifically the financial services industry, which is a global leader in the use of information systems. These systems function at a level where they can be highly effective tools with the right partnership arrangements. Border and immigration systems, by contrast, are owned largely by federal government agencies that have been chronically underfunded, with the participation of an airline industry in financial crisis, and other private sector partners not yet engaged.

3. Generating knowledge about terrorist mobility tactics through information analysis

Useful knowledge about terrorist mobility includes such topics as terrorist group passport practices and likely terrorist choices among

alternative entry channels. Statistics, entry data, and investigative files must be analyzed to produce this type of knowledge. To reach conclusions about risks, they need to consider information at three levels of certainty:

- Known methods of terrorist travel, based on all-source analyses of entry, investigative, intelligence, and open-source information;
- Suspected methods based on current information; and
- Potential methods, based on informed “best guesses” of terrorist tactics by terrorism experts, as well as on successful methods that nonterrorists are known to use.

Known mobility methods. Actual terrorist movements (as discussed in Part I) can be broken down into constituent channels, an analytical practice in keeping with classical intelligence practices and not differ-

Terrorists and the Illicit Travel Market (Europe)

Systematic compilation, analysis, and reporting of terrorist mobility information derived from investigative and intelligence casework—including producing an annual all-source threat assessment—are critical to developing effective terrorist mobility countermeasures.

To what extent, for example, do Al Qaeda and similar terrorist groups outsource their requirements for documents—passports, visas, travel stamps, identification cards, and supporting documents? European-based travel facilitators and criminal vendors of travel and identification documents appear to comprise a significant source for terrorists.¹⁵ An illicit travel document market in Thailand has been the source of supply for at least one Al Qaeda-linked operative, Hambali. Belgian, French, Portuguese, and Spanish passports are frequently seized in Bangkok; the alleged leader of Jemaah Islamiyah, and Bali bombing mastermind, was arrested there with a forged Spanish passport.¹⁶ Since we know the 9/11 hijackers drew on internal sources, information like that highlighted on the map at right may suggest that Al Qaeda and related networks’ recourse to the illegal market derives from diminished internal forgery skills, unavailability of certain documents from previous sources, and possibly a heightened need for documents for complex operations.

ent from mapping terrorist funding channels. Creating a list of known terrorist organization mobility methods by type and frequency is the first basic step in developing knowledge of terrorist mobility. Knowing what terrorists have actually done is immediately useful for instituting new protective practices (e.g., extra scrutiny of particular types of passports on particular routes or of a visa category) as well as potentially for modifying regulations and proposing new laws. Al Qaeda learns from failures and develops new and improved operations; therefore, known practices can also be a guide to predicting future practices.

Suspected mobility methods. Actual warnings through intelligence or law enforcement channels are receiving intense attention daily. These can lead to making a priority of plugging particular holes in the system that might otherwise not have been addressed. Reportedly based on explicit warnings combined with long-term accumulated infor-

Terrorists and the Illicit Travel Market



Source: See footnote 15.

mation about past practices, in 2003 DHS decided to end at least temporarily the “Transit Without Visa” channel until security standards can be improved.

Potential mobility methods. Potential methods of terrorist entry can be anticipated by taking a general approach—vulnerability assessments—or a particular approach—“red teaming” that uses small groups of experts to anticipate terrorist group thinking. Estimates can be enriched by doing a better job of capturing the knowledge of front-line officials.

Red-teaming. “Red-teaming” techniques are the military and intelligence community’s longstanding method of anticipating enemy methods and targets through exercises in viewing the United States from the enemy’s perspectives. Red-teaming, called for by the *National Strategy for Homeland Security*, must be applied specifically to entry and embedding tactics.¹⁷ Suppose you were Al Qaeda leadership, what method of entry and residence would you select? Establishing a practice of conducting these exercises with intelligence professionals is an essential ingredient to border and immigration management risk assessment.

Economists and sociologists can forecast migration patterns and anticipate surges based on observable crises. Law enforcement officials and others can predict and observe how Mexican and Central American laborers may be affected by new border barriers. Terrorists are few in number and hard to spot, and change and evolve their plans to adapt based on the outcomes of previous attacks, to take advantage of newly perceived vulnerabilities, and to up the psychological ante. Red-teaming that incorporates mobility considerations is necessary because information on terrorist intentions and the mobility channels likeliest to be selected can never be complete enough to predict all contingencies. These exercises are not fool-proof, but then no approach is fool-proof.

Vulnerability assessment. Knowledge about vulnerability has become an important factor in homeland security decision-making, but “vulnerability assessment” has two distinct meanings: first, an assessment of the scale and scope of the destruction and damage caused either by

attacks on travel and transportation facilities—airplanes, subways, trains, busses, and highways—or by their exploitation in carrying out a terrorist attack in the United States; second, an assessment of the ease with which terrorists can attack or exploit a particular travel facility, process (e.g., passport acquisition), system (small boat), or particular checkpoint (a given port of entry) for use in traveling and mounting attacks.¹⁸ “Black-hat” teams to test defenses are one tool of the second kind of vulnerability assessments.

Vulnerability assessments in the first, and original sense, are an essential tool for setting priorities for homeland security critical infrastructure protection. Vulnerability assessments that chart weaknesses force our government to take a hard look at our systems and policies. In the mobility context, policy discussion has tended to emphasize the pervasive vulnerability of all of our border and transportation systems by invoking the image of the large number of migrants in the United States without legal status and the methods they have used to enter and remain here. This large population does raise concerns about our approach to security. But global terrorism networks’ mobility practices will have only some features in common with migration practices. Setting counterterrorism priorities for addressing vulnerabilities requires cataloguing known terrorist methods and taking into account expert red-team anticipation of likely terrorist mobility methods. Thus, authorities responded rapidly to a terrorist threat concerning the “Transit Without Visa” program at airports, although doubtless more economic migrants continue to enter through land channels.

Capturing front-line knowledge. Front-line officials often are experts in their field, through experience, training, and sometimes also formal study. Visa officers, field agents, and inspectors are usually the first to spot patterns of anomalies or the latest illegal tactics. Often, they are not heard, especially on the viability of particular solutions. Historically, their knowledge often has been overlooked because the core duties of front-line personnel are to implement border laws—issue visas and check passports—not to systematically collect and transmit information. (Pre-9/11 attitudes toward the competence of immigration officials are discussed in Part IV.) Thus, the critical value of the experience and knowledge in the field is often ignored or lost.

The central orientation of front-line border officials toward implementation contrasts with the orientation of the intelligence community, whose field agents' primary duty is to collect and transmit information from which reports are generated and supplied to analysts, who in turn produce reports for policymakers. But classical enforcement and analytic practices consist mainly of case-specific investigation by agents and

Immigration Statistics Relevant to Terrorist Mobility

Terrorists comprise only a small fraction of the millions of people exploiting legal and illegal immigration channels, but they can easily hide in larger populations of refugees or other migrants. Therefore world migration flows are one important context for assessing potential terrorist pathways. Reasonably accurate information about how many people are coming into the United States, from where, and through which ports of entry or by which geographic route provides a necessary context for any consideration of terrorist entry to the United States. Accurate US immigration statistics systems are therefore central to accurate terrorist mobility threat assessments.

The immigration statistical reports most familiar to the immigration policy community and media are the regular reports on the number of people by nationality apprehended by the Border Patrol along the southwest border. Unfortunately, these reports do not include even statistical estimates of the *actual* number of entries or individuals in illegal channels. This rudimentary level of reporting is insufficient for policy formulation involving immigration and terrorist mobility strategy.

In the counterterrorism context, knowledge about the flow of people into the country is indeed a national security requirement and essential for developing a risk-based terrorist mobility strategy. The intelligence community has occasionally filled in the vacuum in basic migration and immigration statistics. However, it would be more appropriate and useful if DHS published its own annual estimates of the number of people entering the country illegally and identified the geographic pathways. Ensuring support for this reporting seems an appropriate role for the NCTC in its intelligence management role, since accurate information is an essential foundation for strategic operational planning.

officers, and data being pushed or pulled into dedicated units for statistical and/or qualitative analysis. It does not capture what border officers derive from their cumulative experience and daily observations, or what they encounter when implementing new procedures.

The well established methods of developing knowledge through standard intelligence and investigative methods should be supplemented by doing a better job of capturing the knowledge of front-line officials, and making it available to their colleagues and to policymakers in usable form. Qualitative input from investigators and analysts, complemented by statistical analyses, is essential to ensuring that we derive benefit from and actually institutionalize best analytic methods and insights. A kind of “reverse engineering” will enable front-line border and immigration personnel to be *directly* involved in the analytic and problem-solving process.¹⁹ Through a regular and formal process, front-line officials can provide:

- Detailed accounts of emerging illegal techniques they observe;
- Descriptions of the precise steps they took to uncover them;
- Suggestions of methods of countering and reversing these practices;
- Identification of organizational barriers and/or resources that are creating the problem or blocking its solution; and
- Critiques of suggestions made by others about countermeasures.

Debriefing front-line officials requires sensitivity. It needs to occur in special groups using procedures that protect them from retaliation by managers whose roles they may critique.

4. Communicating knowledge to the front lines and to policymakers

Historically, the intelligence community focused on reports to policymakers, and law enforcement agencies avoided reporting. Since 9/11, there has been considerable attention to dissemination of warnings. But there has been less attention to coordinated responsibility for reporting on and communicating analysis of information that can lead to improvements in systems, rules, and investigative focus. A plan for report production allocating responsibility among various agencies needs to be developed, to avoid a miscellany of overlapping reports that do not necessarily address all the pertinent questions.

Some reporting requirements are clear. A series of publications describing mobility channels is a basic requirement for front-line officials as well as policymakers. Mobility channel reports must be reliably frequent and have a standardized, incrementally improved format so that a baseline is established and trends and patterns can be observed—and acted against—over time.

Lessons learned from the 9/11 attacks included not only that the intelligence and law enforcement communities did not “connect the dots,” but that many senior government leaders and the American public never learned the big picture about Al Qaeda’s capabilities and intentions, despite a series of attacks. In the case of terrorist mobility, there is a big picture as well. This big picture of transnational clandestine movement must be developed fully, in a deliberate, continuous, and formal manner, with the full resources of the intelligence, law enforcement, and border communities contributing to it.

5. Integrating mobility knowledge with policy and operations

Mobility knowledge has to be integrated with a range of policymaking and operations from border adjudications, to civil and criminal enforcement, intelligence, diplomacy and foreign assistance, and military operations. Concretely, this means processes like creating electronic systems to flag certain types of passports; proposing new rules to safeguard passport issuance in the United States and in other countries; and working out arrangements for enlisting state and local officials in constraining terrorist mobility.

Drawing on a rich information and reporting regimen, our border, immigration, and transportation systems can be better secured over time. The Visa Waiver Program is an example of the way in which improved information must be continually integrated into policy. With new information, new conditions can be imposed and others adjusted. For instance, information that Al Qaeda has relied on the use of lost and stolen passports should lead to increased focus on obtaining lost and stolen passport data for use in border screening, and that emphasis should lead to consideration of reporting lost and stolen passports as a condition of Visa Waiver Program participation.

We are at the beginning of creating a broader US and global terrorist mobility agenda, already significant even if it is not labeled as such. It includes the massive new border information programs described above (which are part of a larger screening architecture), foreign and military assistance relating to border controls, a series of actions to plug specific holes based on suspected terrorist actions, and an initiative to deny visas to corrupt border officials as a deterrent measure, as well as a long list of other initiatives. Broader and deeper terrorist mobility analysis and reporting should result in this agenda growing in prominence and impact.

6. Knowing what is working to inform improvements

Results matter for effectiveness and fairness. Knowing when an algorithm built into a screening system leads to too many fruitless delays, designing new reports, moving from tightening student visa criteria to expanding the number of student exchange program slots, increasing penalties or enforcement resources—these types of changes should become routine based on ongoing monitoring of what is working in border and immigration system efforts to constrain terrorist mobility.

Actually looking at how an agency is being successful or not in carrying out its mission is not a well accepted practice among civil and criminal enforcement agencies. But we must demand that agencies use information to reassess objectives and practices. We can only know if what we are doing is effective by having baselines, benchmarks, and evaluations. There must be simple, clear, regular reports on the number of terrorist-related suspects denied admission, by location, informational basis for denial (name, biometrics, demeanor, interview, documents, tip, etc.), and legal basis for denial, combined with any verification information. What percentage of terrorism suspects intercepted at the JFK or LAX airports were later able to be confirmed or not as terrorists, and how were the initial and final determinations made? What ongoing information are we using to evaluate the relative risks posed by entry from Canada, Mexico, Europe, and by sea? Using this kind of routine but deep data, officials can improve plans, operations, deployments, training, and technology support, and policymakers can evaluate the costs and benefits of particular policies.

Establishing a dynamic knowledge agenda that reliably acquires and analyzes critical information; combines different kinds of knowledge to make operational plans and judgments about priorities; and makes reassessments without falling prey to initiative fever, tactical fads, or political distortions is the first and most fundamental challenge for a terrorist mobility strategy.

B. Targeting: Terrorists Who Act as Travel Facilitators

By now we are familiar with the drug trafficker, the domestic gun trafficker, and the international arms smuggler. We are beginning to pay more attention to the smuggler of weapons of mass destruction. And we must pay more attention to the fact that Al Qaeda, as part of its formal organizational structure, has had specific individuals whose role was to act as travel facilitators. Just as the government makes a dedicated effort to disable terrorist leadership cadres, it could also make special, priority efforts to disable terrorists who facilitate travel for groups, cells, and networks.

Members of terrorist organizations who act as travel facilitators are important targets for identification and 24/7 tracking and lawful arrest, detention, and prosecution for several reasons. First, they are critical to the immediate, day-to-day functioning of the terrorist network and an essential source of expertise and resources for actual terrorist attacks. Second, terrorist travel facilitators are equally important to counterterrorism for their role as a hub for contacts that provide clues to other aspects of terrorist organizations and operations. As such they are potential targets for broader intelligence collection. Third, disruption of travel facilitator terrorists can precipitate a shift to the use of the existing criminal infrastructure that supplies documents and other travel services to human smugglers and traffickers in people and illicit products. As a focus for disruption, the networks of illegal travel service providers may be more diffuse than a single organizational target, but they may also be more accessible. Their document forgers, procurers, and human and other smugglers are in the illicit business for money and as such are potentially more easily found and deterred from transactions with terrorists than individuals adhering to an ideology. (Attacking illicit travel networks is discussed in Subsection C.)

Tactics against travel facilitator terrorists pose difficult practical dilemmas and legal problems because of their twofold importance for immediate disruption and as sources of longer term information. On the practical level, a decision to disrupt a travel facilitator (by arrest, detention, or death pursuant to the laws of war) sets up the risk of substitution by an unknown successor and that what is now an accessible hub of contacts will not be replaced by one that is also known. A preferable option may be to track the individual, their activities, and connections for the ultimate purpose of closing down those connections and catching the terrorists who use these travel channels. On the other hand, eliminating the terrorist travel expertise could cause a problem for the organization in replacing it and therefore slow down operations. These dilemmas require centralized discussions and resolutions.

The same legal issues that surround actions against all terrorists in foreign countries, especially off the conventional military battlefield, apply to actions against terrorist organization travel facilitators. Frameworks for finding, apprehending, and taking legal action against terrorists outside the United States are in an unsettled state and compel further attention.

C. Crime Control: Attacking Illicit Travel Networks

Terrorist organizations have links with human smuggling networks and other criminal networks whose business is to facilitate travel for trafficking in proscribed drugs, arms, or money, or smuggling ordinarily lawful consumer products. The illegal market in travel services, including criminal exploitation of law-abiding travel agencies, is a problem for transnational crime control and an urgent and important focus in support of a strategy to constrain terrorist mobility.

The Al Qaeda network has handled travel arrangements using internal and external resources, the latter encompassing everything from petty criminals (responsible for a single passport theft) to major organized transnational networks. In some instances, terrorists themselves have used the illegal document trade as a source of funds, which means that criminal investigations can result in uncovering a terrorist. Other terrorists have purchased services from petty criminals, so that, again, an investigation or arrest of a thief may provide a link to a terrorist.

The larger picture is that facilitating illicit travel is a multibillion dollar global industry—one which terrorists can and do exploit. It encompasses criminal networks—of document forgers and procurers, human smugglers and traffickers, and front companies or other institutions that recruit and sponsor migrants for profit—who may also do business with terrorists. The companies procure fraudulent documents for purposes of exiting a foreign country and for obtaining visas to the United States, sometimes in coordination with related entities here. Travel and transportation businesses can be witting or unwitting participants. Illicit travel entities may also be involved in identity theft. Corrupt government officials play a critical role: providing official passports outside of legal channels, supplying a passport stamp for travel that didn't happen or omitting a passport stamp, and facilitating human smuggling. Crime and corruption may be more prevalent in failed or weak states or those where the society is infected with a higher degree of corruption, but they are problems everywhere to some degree.

Any given organization or person of interest may be strictly foreign, have ties and interests that span from foreign locations to border points, or from foreign points to the border zone transit points and further to domestic locations, or be strictly involved in domestic travel and transportation. Thus, there may be a US front company owned by the same individual as a front company in a foreign country, a transportation company that makes border crossings, or an internal travel or transportation company involved in migrant smuggling that has been exploited by terrorists.

Given this range, a key job for terrorist mobility information assessment is to characterize this wide-ranging market in the terrorism context—whether it is diffuse or centered in certain locations, how it intersects with arms and other traffickers, and the role of unwitting agencies. Assessments must move reports based on individual cases to systematic studies that establish baseline information and track practices and trends, including prices in the illicit travel market.

Today there are integrated, multidimensional strategies in progress against human trafficking, and against the nexus of banking, money laundering, and terrorist finance. Policies and programs against human

trafficking, especially involving women and children, for example, are a mix of intelligence and information collection and analysis; investigation and law enforcement; regulation; policy research, analysis, and reporting; and international diplomatic efforts. A comparable aggressive, integrated multipronged strategy—one that goes beyond traditional law enforcement—needs to be developed against the criminal market in illegal travel-related services, and its terrorist links.

A well organized US domestic program, a Western hemispheric focus, and a global dimension to the effort are all needed, and they should be linked. At home, the gap between the demand for workers and the legal supply of them is being exploited by criminal organizations that facilitate illegal immigration. Closing that gap between supply and demand will reduce this market. To the extent that the United States can assist foreign nations in making the illegal travel market less accessible to and reliable for terrorists, obstacles to terrorist mobility are raised.²⁰

Three tracks for attacking illicit market support for terrorist mobility are important:

1. Deterring global illicit travel networks from providing services to terrorists and gaining information from them

An ongoing objective given high priority should be denying terrorist access to the networks outside the United States used by migrants and criminals that terrorists may also be exploiting, including to reach jumping off points to the United States. We should be pursuing a range of actions. Among them:

- The United States should build security partnerships to focus investigative and intelligence resources on human smuggling networks in Latin America in which Urdu, Pashto, Farsi, Arabic, and any other languages immediately relevant to Islamist terrorism are spoken. A counterargument to attacking human smuggling networks as a means of deterring terrorist movement is that targeting the networks trafficking in narcotics has been unsuccessful in stemming supply. Where we have successfully attacked cartel kingpins, a large, diffuse, and even more violent network has sprung up to compete in replacing them. But the “market” in Latin America for supplying terrorists

with access to the United States is not the same as the illegal drug market: there are not legions of users calling forth a practically unlimited population of potential suppliers, at least not human smugglers in Latin America with relevant language skills. Networks in which the languages of Islamist terrorists are spoken in this hemisphere are likely to be relatively finite and should attract special attention. Even if we are not successful in eliminating them, we can likely deter at least some terrorist links through crime control measures, acquire intelligence, and degrade capabilities.

- The Human Smuggling and Trafficking Center (HSTC) should be built up as an all-source, centralized, strategic and operational information acquisition and analysis effort against smuggling and trafficking networks with a dedicated focus on the detection of terrorist links. The 2004 intelligence reform legislation mandated that the HSTC serve as an intelligence fusion center and information clearing house for all relevant information from *all* federal government agencies. However, the government's efforts to address terrorist mobility, human smuggling, and human trafficking have not taken full advantage of this institution.²¹ The lack of sharing of criminal investigative information is a particular problem. The current practice—to preserve terrorist mobility information in prosecution files where it remains inaccessible for compilation and analysis—stands in the way of effective crime control and counterterrorism.
- There should be a well supported, centralized interagency program to find and act against all known individuals and organizations that facilitate travel and have links to or are immediately accessible to terrorists. An intelligence program by the HSTC is a first step; that intelligence must then be acted upon through a substantial, dedicated operational program. Authority to activate these investigative and/or intelligence resources should be attached to the lead entity for this program, likely the HSTC. The HSTC's priorities must be determined by its participating operational agencies and implementation of the NCTC strategic operational plan for counterterrorism.²²
- Finding new means to deter criminal and unwitting travel facilitators from establishing links with terrorists should become a goal.

- Efforts should be made to reach the sources of terrorist travel facilitation. For instance, classic law enforcement techniques should be used to exploit criminal networks, like buy-bust type tactics in which low-level human smugglers are arrested in stings and returned to their organizations in return for providing information about routes and potential terrorist links.
- To increase law enforcement pressures on transnational criminal organizations, cooperative legal and operational structures should be established with foreign governments. These range from law enforcement, to diplomatic initiatives, to formal agreements and new treaties. As a start there should be a dedicated Terrorist Travel Operations Unit for extended and short-term postings abroad to support cases with a US nexus and wholly foreign cases that have the potential to have a US nexus, such as smuggling from South Asia to Europe.

Information about foreign travel documents that emerges in criminal investigations can support a broader terrorist mobility strategy. For example, when Al Qaeda precursor El Sayyid Nosair was arrested in New York City, he was found to have multiple Nicaraguan passports. They were obtained after the major earthquake in Nicaragua, which required a large number of passports to be reissued, resulting in loosened controls. Sharing this information with immigration regulatory authorities would enable them to build in systemic alerts for similar passports—electronic programs for front-line adjudicators—and to develop proactive programs. For example, the experience with Nosair might lead US diplomats to target some post-disaster assistance at preventing the weakening of passport issuance controls.

2. Detering illicit travel networks in the United States from providing services to terrorists

Prosecutions against document rings and human smugglers aimed at the United States have more prominence than before 9/11. But prosecutions for travel document fraud should still be given higher priority. The lead investigative agency, Immigration and Customs Enforcement (ICE), requires a dedicated terrorist travel program. As with terrorist finance investigations, classic case-by-case, field-driven law enforcement is important but only a part of what is needed. ICE's internal analytic unit

should be able to access open-case file information for analysis of tactics relevant to terrorist travel and have a lead role in the Human Smuggling and Trafficking Center. Centralized collection and analysis of travel documents obtained from terrorism suspects and related interview information would add invaluable new information and perspectives.

Moreover, deterrence in the terrorism context has yet to be seriously explored. We should be asking how we can deter criminals from interacting with terrorist organizations, and how the goals of deterrence and gaining information can be combined—for attacking both the domestic and international illicit travel markets. Strategies of “group deterrence” pioneered in the mid-1990s and used to reduce youth gang violence may be suitable for adaptation to counterterrorism in the context of enforcement action against human smuggling and trafficking networks. In contrast to a kingpin strategy, which focuses on arresting leaders to dismantle or debilitate criminal organizations, group deterrence aims instead to stop groups as a whole from engaging in a particular activity, for instance from using violence or setting up open-air drug markets. The strategy holds all members of a group accountable for individual members’ violations. Smuggling networks should learn directly from authorities that links with terrorist organizations will result in priority dismantlement of the organization. This approach is only possible if there is a foundation of comprehensive intelligence about networks and their members.²³

3. Intensifying domestic and international action against all illicit travel networks, even those without any apparent nexus to terrorism

Whether or not it is possible to deter criminal networks from dealing with terrorists, pressures on criminal organizations involved in illicit travel and smuggling generally should be stepped up. The market in clandestine travel services will exist as long as there is crime and migration outside of legal channels. But we must use immigration policies and law enforcement to reduce resources available to terrorists, as well as the violence and crimes these networks facilitate. A wide range of governments, and of law enforcement, communications, regulatory, and diplomatic tools can be brought to bear. Reforming US immigration laws to lower demand for services in the illegal travel market supplying access to the United States is discussed in Subsection F below. But in addition to adjusting our federal immigration laws to permit more order-

ly legal migration, we must also be more effective in enforcing laws against large-scale criminal violators.

- We should give a higher priority to diplomacy leading to bilateral, regional, and international agreements and treaties to raise the worldwide level of enforcement against crimes that involve exploiting immigration, border, and transportation systems to carry out terrorist acts and major crimes. At a minimum, our diplomatic agenda must include the imposition of adequate legal penalties supported by adequate enforcement resources in states allied with the United States against terrorist organizations, covering the full range of travel crimes that enable terrorist mobility, from passport forgery and theft to human smuggling. These agreements should build on existing counterterrorism and migration agreements, beginning with the former. Where governments, especially in developing countries, may view human smuggling as a means of relieving internal political pressures, attention to those problems in the context of a common threat from terrorism or crime increases the likelihood of gaining meaningful cooperation.²⁴
- There should be significant programs to prevent and detect corruption in US border services, including research, analysis, new preventive policies, and enforcement.
- The United States could expand its international anti-corruption policy efforts to incorporate a specific effort against travel facilitators—passport officials, customs inspectors, airport officials, and immigration judges. This would include a more prominent public focus on the problem, specific reporting, regulatory and legal reform, and other foreign assistance related strategies.

These measures complement legal and diplomatic efforts the United States and security allies must make to secure legal entry channels and to deny access through illegal channels—for example, securing passport issuance channels, upgrading travel document security, developing effective border controls, strengthening airport inspection regimes, ensuring the integrity of birth certificates and other identity documents, securing biographical and biometric records, and so on.

Terrorist mobility is woven into the movement techniques of global criminal organizations, which have significant resources to spend on clandestine movement. Regardless of what aspect of the system is involved, facilitating terrorist travel represents a greater threat to the United States than drug trafficking. The objectives set and the resources provided against travel facilitators and their organizations should reflect that reality.

D. Global Awareness: Tracking Terrorists *En Route*

Beyond disabling travel facilitator terrorists, we must strengthen our ability to identify and track *any* individual or small group of terrorists on the move. This is essential for providing warning and being prepared to respond to threats, but also for our global strategy. States whose officials provide travel documents, safe passage, or safe haven must become the focus on diplomatic intervention and terrorism policy.

The tracking mission begins as soon as strategic analysts in the counterterrorism community have identified the emergence of a terrorist threat. We want to be able to track individual terrorists specifically to intercept terrorists aiming at the United States and US targets abroad, and as part of a global effort to constrain and deter them. The more individual terrorists' movements are understood, the greater our ability to design arrangements to close troublesome pathways.

As the history of the intelligence community's knowledge of Osama bin Ladin's movements prior to 9/11 shows, tracking important individuals using every available means is a longstanding practice. But it has been expensive and difficult to track individuals on the move transnationally given constricting legal frameworks, governmental resources and organization, and technological tools. Close tracking therefore has been historically limited to individuals considered highly valuable—leadership cadres, financiers, and those potentially aiming at the United States. (Travel facilitator terrorists were not *per se* in this league.) As the 9/11 episode shows, there were organizational and management weaknesses even in the tracking efforts undertaken by the intelligence and law enforcement communities.

Expansion of terrorist tracking and investment in new techniques are clearly growing. Brief consideration of two new directions in this effort—new alliances and new technology programs—will serve to highlight the different demands of terrorist mobility tracking and immigration policy.

New alliances. A basic fact for the United States in tracking terrorists—in contrast to monitoring the movements of Soviet and Soviet ally armed forces—is that they are mingled in the populace of states, including those who are our security partners against terrorists. Conducting unilateral counterterrorism operations that violate the laws of foreign nations to gain information or take action, even against terrorists, risks our alliances, credibility, and ultimately, legitimacy as a nation of laws promoting democracy. On the other hand, increasing our ability to find out where terrorists are and to disrupt them—whether through criminal justice systems or otherwise—is essential.

The practice of rendition has been perhaps the most notable example of exploiting terrorists' travel outside of their countries of citizenship. During the 1990s, arrest warrants issued by nations other than the United States provided at least a partial legal footing for at least some of the US government's practice of rendition: participation in tracking, enticing or capturing, and bringing or "rendering" terrorists from one foreign nation to another foreign nation that had issued a warrant, an operation substituting for an extradition proceeding that may not have been available. While the full history of these actions has not been published, it appears that rendition has been successful in capturing some dangerous people.

But rendition—as a potentially lawful arrangement by a consensus of three or more nations—remains a tactic under a cloud for several reasons. Initially it was disparaged as mere case-by-case enforcement, inadequate as a counterterrorism measure after 9/11. Critics contrast the efficacy of case-by-case rendition with military action against Osama bin Ladin's forces and the Taliban government or the war in Iraq. The suspicion that the US government has used rendition, as well as *refoulement* of detained US residents, to bring about the use of torture and other forms of coercive interrogation illegal under internationally accepted law has also tainted the practice.²⁵ Also troubling is the possibility that the

government may have made significant mistakes in its targeting, causing significant harm to a number of individuals, without any political or formal accountability for their suffering or for improved government performance.²⁶ Finally, post-9/11 renditions that may be carried out on an extraordinary basis without notifying the host government highlight domestic problems in gaining consent for new forms of counterterrorism and potentially undermine our legitimacy as a security partner.

A multistate counterterrorism effort must involve a lawful method for rapid disruption of known dangerous individuals as a crucial component, and it must be recognized that at any given moment the dangerous individuals may be outside of the nation to whom the greatest threat is posed and outside their nation of citizenship. Going forward, we must pay greater attention to the legal foundations for this program, including in shoring up or devising new kinds of extradition agreements among states.

The United States is already expanding the scale and efficacy of tracking terrorists through collective efforts with Atlantic and other allies at a network of joint operations centers called Counterterrorist Intelligence Centers.²⁷ For example, an intelligence community Alliance Base in France has been established from which to track terrorists. Because the United States has joined forces with France and Germany in addition to historical English-speaking allies, the chances for and scope of successes are greater. Such bases add resources to efforts the United States might otherwise have had to make on its own; develop new opportunities the United States may not have otherwise known about or acted upon; and provide a context for allied governments to begin to resolve some of the legal impediments to operating extra-territorially by establishing a consensus *modus operandi*, at least among these participants.

Seen as a successful pilot program and embryonic legal arrangement, this effort could provide an impetus for the growth of other more formal cooperative structures. To operate jointly, the parties need a set of rules, and these rules serve as operational and legal demonstrations and precedents. In the longer run, the network could evolve into an effort to establish a series of jointly operated or supported terrorist information points that capture transit information or involve actual arrests at key global transit points into collectively secured space.

Notable about the arrangements that have been publicly reported is that we do not have formal agreements with these nations to share information for terrorist or criminal watchlists. The immigration, customs, and border control agencies that can best exploit watchlists have historically operated in separate realms from the intelligence services that would staff a base for allied intelligence operations. But terrorist watchlists, in addition to being potent tools to enable defensive detection at border and transportation access points, are also potentially a major source of information for offensive terrorist-tracking and terrorism analytic units, because border officials may pick up on terrorists not already being tracked by intelligence operatives.

It would be a significant step forward if the same countries that can cooperate to share intelligence in *selected* cases could use the same cooperative setting to find a legal framework in which each country's *entire terrorist watchlists* could be available for use—with appropriate safeguards—by the tens of thousands of border officials. Absent mutual watchlist access, the border services of one state participating in Alliance Base can be admitting another's citizens placed on a watchlist by their home government as known or suspected terrorists or criminals. At the very least, it would seem that the other security service would want to know. Regardless of who takes the lead in cutting this complicated set of Gordian knots—which implicate the rights of suspects, informational privacy, and intelligence sources and methods—it should be a major goal to move from sharing information in selected high-value target cases, to collective establishment of globally criss-crossing terrorist tripwires through jointly established terrorist rendition attraction points and shared border watchlists.

Research and development. During the Cold War, the United States ensured that movements of enemy armed forces were visible to the government through substantial investments in satellite technology and other collection practices over decades. Although the government suffered some strategic surprises, a formidable array of tools—collection of information and intelligence, analysis, technology supporting collection and analysis, and ongoing reporting to policymakers—largely kept the Soviet Army's movements visible to US political leadership.

Finding and tracking terrorists has largely been a matter of a combination of intelligence collection using technology developed for the Cold War and law enforcement investigation with little computer analytic support and limited involvement of border officials. Our tools for detecting, collecting information about, and analyzing movements by conventional armed forces are inadequate for finding or anticipating the movements of terrorists or global criminals. Communications technology remains relevant, as does the intelligence community's experience with undercover identities and clandestine border crossings, and existing border control and enforcement systems aimed at terrorists and criminals. But although the US military and its private sector technology contractors have made striking advances in using electronic communications to track rapidly unfolding events on a conventional battlefield, our national security services so far have been unable to apprehend Osama bin Ladin.²⁸ Since small groups of terrorists are posing a major threat, tracking such groups and individuals needs to be reconsidered to see if new technology, as well as new alliances, can increase the visibility of single adversaries.

One major approach, discussed in Subsection E below, is for the United States to make a more systematic and global effort to work with allies in equipping nations that cannot afford screening systems with the necessary tools to secure legal entry channels and detect known and previously unknown terrorists. But it is important to think out of the border control box as well. For example, could the United States work with allies to gain legal access for security officials to the international transportation reservations systems? Australia requires travelers coming to Australia to obtain a visa through the airline reservations systems. That is, a request for a reservation is automatically transmitted to government authorities, who then screen the request and advise the airline whether a reservation may be granted. Other nations, including the United States, have also looked at the problems of instituting such a system. If we are facing a type of enemy that poses a threat to people in numerous nations, and to the functioning of the international transportation systems on which we depend, something more flexible and global than the Australian system also seems to be required. Nations participating in a global alliance against terrorist groups should be able to share information at all times from a system tracking watchlisted individuals, consistent with privacy norms and law.

E. Border and Immigration Management: Securing Legal Entry Channels

From the viewpoint of counterterrorism, counterespionage, and law enforcement authorities, the borders of states have historically presented rare opportunities to detect and intercept adversaries, who are forced to surface at this point and engage with governmental authorities. When terrorist adversaries transit official access points they must take measures to conceal themselves that provide governments and their security partners with opportunities to detect and disrupt them. Legal entry channels—visa offices and official ports of entry at land, air, and sea access points located before and at national frontiers—are therefore newly critical infrastructure for counterterrorism. They are also critical for responding to pandemics and other security threats and for the safe and efficient management of trade and travel.

Securing legal channels from terrorists and other threats through a “smart borders” policy that relies on modernized infrastructure to make use of foreign and domestic intelligence about terrorists, as well as on risk management tools, has been a cornerstone of homeland security strategy since shortly after 9/11, when it was discovered that at least two of the hijackers could have been, but were not, tracked and placed on the terrorist watchlist designed and used by border authorities.²⁹ Pursuant to this strategic vision, steady improvement is being made in the complex task of equipping visa offices and ports of entry for more comprehensive and efficient screening of applicants for entry.³⁰

But we are far from sufficiently exploiting opportunities for disrupting terrorists in legal entry channels. Part of the reason may be overemphasis on the terrorist watchlist as a model of interaction between the intelligence and border authorities. The watchlist model leads to an oversimplification of the task of countering terrorist mobility in legal channels.

Consistent with repairing the notorious failure of the intelligence community to track two of the 9/11 hijackers and detect them when they applied for entry in Los Angeles, the basic post-9/11 framework for preventing terrorists from attacking in the United States has been a three-

fold: offensive counterterrorism overseas using intelligence operations and war, run by the intelligence and military; defensive “smart borders” using intelligence and tightened immigration procedures to screen travelers combined with a better patrolled national perimeter, run by DHS; and a domestic counterterrorism program relying on improved intelligence and antiterrorism law enforcement, run by the FBI. No matter what we do, some terrorists are likely to successfully enter the country and attack again, so national homeland security strategy also calls for DHS to work with the private sector in reducing the vulnerability of critical infrastructure to damage from attacks; for special focus on catastrophic threats like bioterrorism; and for working with the Department of State and local partners to build up our emergency preparedness and response capabilities.

Although the watchlist remains a core element of securing legal entry channels, the initial model of making an otherwise important border and transportation system “smart” enough to detect terrorists through reliance on “intelligence and warning” may be slowing the development of a more comprehensive strategy to disrupt terrorist movements. A view with persisting currency sees actions that border officials themselves take in legal entry channels as ineffectual, unless they either rely on foreign intelligence or constitute tougher “enforcement” leading to the barring of more travelers and immigrants across the board. Thus, with the watchlist fiasco in the background, strategic operational thinking perpetuates a bifurcated security framework that sees “intelligence” as being acquired through classic intelligence sources and methods, mainly abroad, and sees border and immigration management as either passively applying that intelligence or following pre-9/11 immigration enforcement policies, such as seeking to remove all travelers with facially false documents.

This model of securing legal entry channels is anachronistic and leads to a disproportionate emphasis on foreign intelligence as a means of countering terrorist mobility, to the neglect of measures informed by terrorist mobility knowledge and operations concentrated uniquely in border and immigration channels, and to a tendency to look to broad-based immigration reform to do the job of counterterrorism.

We must change the prevailing paradigm. Border officers can no longer be viewed as mere *users* of intelligence gathered elsewhere. They are essential, active participants in generating terrorist mobility intelligence and in exploiting terrorist mobility. But the knowledge they generate and the actions they take do not fit the standard model of classic intelligence functions carried out within the traditional intelligence community.

While watchlist application remains critical, so are the following functions that depend entirely or in part on border officials and their information systems:

- Real-time uncovering of a previously unknown and untracked terrorist through interpretation of clues in travel documents or from an interview, based on other records and terrorist mobility information;
- Post-incident retrieval of an informational footprint for use in terrorism investigations;
- Reduced use of multiple aliases through the taking of biometric imprints that are also useful as a path to other information;
- Data and investigation information collection leading to analysis that reveals patterns and practices of illicit travel and forms the basis for defensive and offensive improvements and operations; and
- Information system design and practice that facilitate sharing among allies, which is essential for tracking terrorists.

All of these functions require a mix of classically collected intelligence information and standard border practices—intelligence, current and historical border data, border experience, regulatory changes, adjudication process changes, and enforcement policy revisions. The protections they offer cannot be drawn simply from foreign intelligence.

For border authorities to intercept terrorists not already watchlisted, traditional immigration adjudication policies must be reconsidered from the perspective of terrorist mobility. Standard adjudication policy, for example, aims to reject any unqualified applicants and send them back to their embarkation point. But although it is infinitely preferable to remove terrorists than to admit them unknowingly, deflection is not necessarily optimal security policy. Without having identified the terrorist, sending him or her back leaves the terrorist at liberty to reveal information about US defenses and continue activities elsewhere. Detection pro-

vides the opportunity for surveillance and its informational fruits, whether in the United States or by arrangements with other governments. Thus, alternative adjudication processes must set thresholds for higher levels of document scrutiny based on terrorist indicators and build in debriefings of people who use false documents that provide trails back to sources and establish pattern and practice information that leads to improved regulatory measures.

Developing the roles and responsibilities of border personnel so they are effectively engaged in what have been viewed as exclusively intelligence and crime control functions will require adjusting training and career paths among border agencies, between intelligence and screening units, and between agencies primarily dedicated to border functions and full-time intelligence agencies. Similarly, to equip border officers and transit points today with the information and process tools needed to attack terrorist mobility can only be accomplished through a combination of *terrorist-specific* tools (e.g., a terrorist travel document capability), and *general* information collection and compliance systems (e.g., establishing a requirement for capturing biometric records of foreign travelers and a system for tracking student visa status) that must be designed for multiple purposes, including counterterrorism.

Since transit points to the United States are located in other countries, which may themselves be venues for attacks on US persons and security allies, we must dedicate much more attention to formal and informal arrangements with other governments to increase common security standards for travel documents, border controls, and transportation. These efforts must extend beyond intelligence organization cooperation to treaties and complementary criminal laws. The United States and other wealthy states also must join together to assist impoverished nations in improving their travel documents, border controls, and transportation security. The long term goal is to create collectively secured legal travel channels just as the terrorist finance and money laundering strategies are attempting to secure global financial systems.

From a terrorist mobility perspective, our goal in securing our own legal channels should be to detect as many terrorists as possible in real time and to reduce vulnerabilities by strengthening systems to deter terrorists.

As is emphasized in the “smart borders” concept, most of the border information systems needed to support effective counterterrorism also contribute to the support of other vital national interests—travel and trade; customs revenue collection; crime control not necessarily linked to terrorism; and an orderly immigration system. Nevertheless, it is time to move to a clearer differentiation of the complex processes and tools required to find terrorists among the larger flow of illicit travelers, so resources can be allocated rationally among counterterrorism and crime control, routine travel and economic requirements, and immigration management.

To achieve this goal, we must identify the *specific* elements we need to detect and record terrorist passage and to deter terrorists—elements that stand as distinct systems and processes, and that are integrated into systems also designed for immigration management and crime control. Below are eight of the elements of an ongoing program combining terrorist-specific and tools of broader applicability needed to secure legal entry channels from terrorist exploitation and attack.

1. A terrorist travel document program. Travel documents such as passports are vital tools of a terrorist mobility strategy because they present a name, and increasingly a biometric identifier, that can be further checked, and they may reveal other important information, such as the individual’s travel history, or whether the document itself is stolen or has been manipulated to falsify travel. Primary border inspectors historically have received alerts about problem documents and may be equipped with special lights for inspecting passports. But overall, far too little attention has been paid to travel documents—the assurance of their integrity, their suitability within national and global screening architecture, and, most immediately, the tools, processes, and training needed to permit their systematic examination for what they reveal about their bearer, their source, and the bearer’s associates.

A travel document program should be established that pursues multiple purposes, among them:

- *To detect terrorists through scrutiny of their documents.* A number of document-related techniques can contribute to the uncovering of a previously unknown terrorist or the confirmation of terrorist identity,

for example: (a) identifying lost or stolen passports; (b) finding counterfeits; (c) spotting unauthorized markings in passports, including counterfeit travel stamps; (d) identifying suspect travel patterns; (e) finding indicators of corrupt passport issuance; (f) finding indicators of corrupt travel facilitation; and (g) finding fraud in supporting documentation, such as foreign identification documents.

These techniques must be ordered into efficient border processes, systematically deployed, and support non-specialists and highly trained and experienced specialists. Some document screening functions should be automated through available computer technology. A challenging task for an inspection program is to establish the triggers for a specialized level of scrutiny of a document found to be fraudulent but which does not have terrorist indicators detectable in the first instance.

- *To assure security for US-issued travel documents, especially passports.* Passports issued within the United States to US citizens represent the gold standard as a mobility instrument. Their issuance should be a focus for the highest security standards. But the full panoply of US-issued documents—including border crossing cards and visas—must be made compatible with interoperable biometrics and adhere to the highest security standards.
- *To contribute to the development of new operational countermeasures by maintaining a centralized collection and/or database of illicit travel documents related to terrorist entries.* In addition to a comprehensive collection of fraudulent documents and/or their images, a computer program at the front lines should perform automated checks against legitimate and illegitimate exemplars.³¹
- *To track problem documents back to their source as part of an operational effort to prevent that source from further supporting terrorist travel.* Information about the source of the document itself is important to an effort to attack the illicit market in travel documents. Sources of fraudulent passports may include public corruption, lack of passport issuance security, a ring of thieves, or an isolated theft, any and all of which may or may not be linked to passports previously associated with terrorist organizations, or otherwise to terrorism.

Identifying documents' sources requires a systematic effort. Over time, border officials could build up information that would allow counterterrorism and crime control officials to identify and put pressure on the illicit travel facilitators behind the intercepted travelers, information that can be combined with investigative information from tracking human smugglers, and intelligence information from special collection and operations against terrorists.

- *To use US influence to bolster travel document security standards worldwide, with priority attention paid to entry from Canada and to Visa Waiver Program countries.* Entry requirements from Canada and Mexico have to ensure that adequate standards of identification are met. Visa Waiver Program requirements should be updated to reflect the increased importance of travel documents in counterterrorism. Participating countries should be required to share information on lost and stolen passports as well as meet increased biometric standards for passports and other requirements set by the International Civil Aeronautics Organization (ICAO) for travel documents, with the United States meeting the same standards. The United States, European, and other Visa Waiver Program countries should jointly develop global security guidelines for passport issuance. For poorer nations, this group must join in a multilateral border control assistance program.

2. A protocol for probing for false personas. Special techniques are required to probe for false personas—terrorists equipped with apparently legal documents but who are not entirely the people represented. As for counterespionage, terrorists armed with legends are now a potential problem for border authorities, who must be concerned about high-level operatives that Al Qaeda or another terrorist organization seek to embed under cover of a legitimate business and visa. Relevant techniques for deep cover protection must be continually improved and incorporated into training for front-line border officials and law enforcement officials. The challenge lies in deciding which applicants require this level of security investment as much as in developing the techniques.

3. A terrorist entry incident reporting program. When an applicant is denied a visa or admission (or admitted under surveillance), the

information should be centrally compiled and used to report to senior managers and periodically to policymakers. Reports should include information such as: who, where, why (watchlist, name-based algorithms, interview, document basis, informant, intelligence), legal basis for denial, personnel associated with attempted entries, and whether terrorism links were confirmed or found to be erroneous. For senior managers and policymakers, knowing how many terrorism-related denials occurred by consulate and port of entry, and something about the circumstances, provides a basis for insights into illegal entry tactics and for making security improvements. Confirmation of the terrorist links of the denied individual is critical for analytic purposes and so that percentages of accuracy can be determined and improved. Such reporting should be aggregated with data about terrorism-related incidents in illegal entry channels for a comprehensive, regularly available, and updated account.

4. Terrorist watchlist improvements. Continuous improvements of the watchlist are essential. Aggressive efforts to break down barriers to information-sharing with other nations, improved technical capacity, linkages with other systems (such as private sector employers), as well as accountability for ensuring comprehensive submissions to the system and for meeting standards for submissions and response requirements are areas that deserve attention.

5. A biometric entry-exit-immigration screening system. The United States requires a basic and continuously improved biometric entry-exit and immigration benefit screening system that can be used with a terrorist watchlist and other sources of terrorist-specific information. Much of the post-9/11 investment in improved screening is directed through the US-VISIT program, which has four stated goals: installing a biometric capacity—to record traveler fingerprints—in existing screening systems; expanding automated screening using biographic and biometric databases; establishing effective checking at exit points; and providing a unified electronic record for noncitizens accessible on appropriate terms by offices throughout the immigration and relevant law enforcement systems.

Although the design of the US-VISIT system originates with immigration control concerns expressed by Congress in the mid-1990s, and funding

for its deployment came after 9/11 in response to terrorism, it is a system integral to a terrorist mobility strategy. Given the scarcity of opportunities to detect terrorists (and major criminals) in free societies, the opportunity represented by the border zone must be maximized. US-VISIT, like other border information programs is best seen as one element of a continually evolving set of border and immigration system capabilities that seek to capitalize on the vulnerability terrorists have while traveling transnationally. Information systems in legal entry channels, including US-VISIT, must transform immigration checkpoints into information-rich environments in order to support effective counterterrorism, crime control, and immigration law compliance and enforcement.

This system should be required to provide a basic biometric entry and exit capability as soon as possible, together with the promised links and single non-citizen file, but we should not expect work on it to terminate. In today's information society—as reflected in the banking system, for instance—critical information capabilities are upgraded on an ongoing basis and repeatedly modified until replaced with new generations of capabilities. Even personal computers are replaced within a few years. What matters for a system's effectiveness at any given moment is whether the current system is the best that it can be, and that it gives the users the opportunity to help make improvements that will lead to the next generation of systems. US-VISIT and the related information capabilities at consulates, ports of entry, immigration benefit centers (and potentially at bi-national facilities within other countries), and related analytic centers must be treated as a dynamic system requiring continual investment to maintain, upgrade, and replace its components.

Considerable skepticism has greeted the scale and budgets involved in US-VISIT, particularly by those worried about DHS's capacity to provide security and maintain the commercial pace that Americans expect and on which our economy depends. The ignoring of long-voiced demands for more border infrastructure to handle the increasing flow of traffic generally—more traveler processing space, roads, and bridges—feeds anxieties. While the *National Strategy for Homeland Security* alluded to projects for large-scale modernization at border crossings, this commitment appears to have been deemphasized.³² Moreover, US-VISIT poses other practical and legal challenges: technical issues in

installing biometrics at land-border exits; privacy protections for data used to screen visitors and US citizens; and security standards for storage of biometric data in the United States and elsewhere, especially in light of the rash of identity thefts we have witnessed in credit card firms and other businesses.³³

We cannot afford to lose focus on what is a critical national security program, however. One of the political disadvantages under which the biometric entry-exit program is laboring is that by the historical standards of investments in automated customs and immigration systems, US-VISIT is a massive and expensive program which presents the kind of serious technological challenge and long-term costs usually associated with military and intelligence infrastructure—and Department of Defense budgets. Terrorist mobility is a challenge arising not only in a military environment, however, but preeminently in the border environment, which, absent enemy states on our borders with armies readied to march against us, also functions as an essential gateway to our economy and society.³⁴ Therefore, costs associated with legal entry and exit channels tend to be viewed more as an aspect of the market economy, not as part of the national security budget and agenda. But the establishment of what the *Homeland Security Strategy* (2002) called “smart borders” to provide security in the environment where travel and commerce take place is fundamental from the perspective of a terrorist mobility strategy, as well as for public health emergencies. With funding for US-VISIT lagging and critics waxing pessimistic about exit controls, this seems not yet to be fully accepted.

The difficulties inherent in US-VISIT and related systems must be faced and overcome. It is fair to assume that bolstering of legal entry channels has already made a significant contribution to national security. Attention has focused on the fact that while US-VISIT’s biometric screening has detected close to 1,000 individuals with criminal histories and/or immigration violations out of tens of millions of travelers, none have been publicly identified as having any relation to terrorism.³⁵ But biometric identifiers, which deter the use of multiple aliases are a significant terrorist mobility countermeasure, especially when they become a part of information-sharing among security allies. Installing equipment to capture ten rather than two fingerprints, as is planned, will enhance

the likelihood of identification tied to latent prints left at crime or terrorism sites—relatively fewer but more valuable. Securing birth certificate systems in the United States and in other countries will strengthen the value of border screening for countering terrorist mobility. Moreover, as our Atlantic allies and other nations adopt their own visa fingerprint systems, a technical opportunity begins to emerge to improve information-sharing about terrorists and criminals in mutually agreed upon legal frameworks. Interoperable biometric systems (internally and externally) and legal frameworks for using them will lift our security to a significantly higher level.

6. Training and specialization in terrorist mobility countermeasures. Even powerful information technology is insufficient without people to use it. More inspectors and more interviewing at the primary inspection posts should be built into the system, with enhanced training and specialization in documents, among other aspects of inspection. Training should be extended to the State Department and local officials and there should be cross-service and cross-training for terrorist mobility experts among agencies involved with border and immigration system security, including any relevant components in the intelligence community.

7. Screening coordination. A major function of developing a strategy for constraining terrorist mobility is to ensure adequate emphasis on coordination and integration. An immediate need is to build up mechanisms for ensuring interoperability of biometrics in the multiple travel documents issued by the US government to US citizens and foreigners and to supporting identification documents also linked to access to transportation and critical infrastructure. Efforts in this direction are being made, and DHS has set up a Screening Coordination Office as part of the reorganization announced in 2005.³⁶

8. Long-term planning and research and development. There is a significant need for long-term planning capacity that designs possible future travel security systems—replacing the inked entry and exit stamp system with an electronic record, a system that would set international protocols for the translation of names in passports, and an ability to build in screening to reservations systems. Substantial planning capacity and

research and development funds have been historically associated with the military and intelligence community; in this instance, the border is the relevant national security environment and these capacities need to be built up at DHS and the Department of State.

During 2005, the political focus for homeland security shifted away from improving security in legal entry channels to controlling migration through illegal channels, especially across the Southwest border. A number of critical counterterrorism elements were deemphasized in the process, including the need for: terrorist mobility knowledge practices at border points; large-scale modernization at border crossings to support a biometric entry-exit system; and secure birth certificates and identification for US citizens and all others crossing our borders. From a counterterrorism perspective, major investment in securing legal channels remains essential because illegal use of legal channels will always be the more attractive option to terrorists. Legal channels pose fewer physical risks than entry through illegal channels—an operative can die in the desert—and afford the advantage of documents that potentially offer the appearance of legal status, thereby facilitating mobility, fundraising, and other planning once inside the destination state. In particular, the most dangerous terrorists—senior level planners and organizers—are more likely to come through legal entry channels presenting seemingly legitimate personas and identities so that they can embed themselves for the duration of planning and preparing for an operation. These senior operatives will be hard to detect upon entry or exit. But some will be detectable and the effort to make this more likely should be recognized as a top priority for policymaker attention and budget resources.

F. Perimeter Control: Denying Access Through Illegal Entry Channels

Infiltration by terrorists through illegal entry channels—avoiding screening by crossing surreptitiously away from a port of entry—presents a worldwide challenge for counterterrorism. Territorial borders between free nations not at war are for the most part unpatrolled except for official ports of entry. Bodies of water between countries not at war are inviting transit zones. Borders controlled by warring factions can be exploited by foreign terrorists. The uncontrolled Pakistan-Afghanistan

border area gives Al Qaeda a notorious haven; in Africa, movements out of terrorist sanctuaries are facilitated by porous borders; in Iraq, fighters cross the Syrian border to join Al Qaeda forces.

Given that our neighboring states of Canada and Mexico are friends, the idea that we might need to control the passage of single individuals or small groups of people back and forth over the entire expanse of our national perimeters still has a ring of absurdity to it. It also has a ring of futility, due to the sheer magnitude of the country and our sense that air and land surveillance technology, fences, and enforcement operations have not proven to be meaningful obstacles for narcotics traffickers, smugglers of cigarettes and other products, and human smugglers and traffickers.

One therefore has to ask at the outset how realistic and significant a threat this kind of remote clandestine entry by terrorists is for the United States. The answer is that it is hard to say with precision, but the possibility cannot be ruled out, so vulnerabilities must be reduced and response capabilities heightened.

From the perspective of today's terrorist groups, since it is preferable to be protected by an apparently lawful visa upon entry through a port than to attempt an illegal crossing, it still seems somewhat more likely that terrorist organizations would seek to place higher level operatives inside the United States through legal channels so that once inside the United States they could look for recruits to carry out attacks. But there has been one prosecution involving a relationship between Hizbollah and a human smuggling organization, and, as has been emphasized repeatedly, revision and flexibility in planning have proven to be hallmarks of Al Qaeda. Prior to 9/11, there was distinctly less risk of detection at consulates and ports of entry than there is today.

Securing legal entry channels has a long way to go, but as the United States becomes more equipped to detect terrorist transit, the risk calculus is changing. Authorities have intercepted a letter, purportedly written by Abu Musab al-Zarqawi, calling attention to the possibility of infiltrating the United States across the southern border.³⁷ Even if it is a second best alternative, reconnoitering and costing out the possibilities

for entering clandestinely by illegal channels based on lessons from narco-traffickers and other smugglers is a plausible option for terrorists. More marginal self-starters who have small-time criminal experience may be more likely to use improvised methods that could involve crossings away from ports of entry.

Moreover, terrorism is not the only context in which remote border crossings may pose a problem for the security of the US population. Sealing US borders and using quarantines may be required during pandemics. Although as a practical matter this may primarily concern ports of entry, contagious disease outbreaks may also require that we be able to monitor our territorial, maritime, and air perimeters.

This conclusion is not new. The initial *National Strategy for Homeland Security* mentions the obligation to “monitor all our borders in order to detect illegal intrusions and intercept and apprehend... people attempting to enter illegally,” within a homeland security framework of allocating resources in a balanced way to manage risk.³⁸ The 9/11 Commission made the point as a matter of counterterrorism.³⁹ The Secretary of Homeland Security has announced the goal of operational control of both the northern and southern borders within five years.⁴⁰

Notwithstanding these declarations, the dimensions of the actual problem are such that they remain a challenge to carry out within a coherent security agenda. Declarations aside, we have barely begun to grapple seriously with the question of how and by whom this is to be done, according to what principles and with what goals, in what time frame, and what the priorities are for immediate action.⁴¹

Without providing answers to these questions, a few general observations may be made that give a sense of the type of discussion and planning needed to address the threat of terrorist entry using illegal channels.

Terrorists may choose among three major alternative approaches for surreptitious entries through illegal channels.

Open stretches of our perimeter present terrorists with three major alternative options for infiltration. One is to enter the United States

(and other democratic and wealthy nations), by mingling in the flow of migrants, refugees, and asylees who attempt entry through illegal channels over northern, southern, and coastal borders. This may mean tapping into the criminal support system for border crossing, smuggling, interior transportation, and documents needed for residence, and using different routes than those used by migrants moving on their own. Or terrorists may make their own probes and find their own routes, far from migrant crossing areas or narcotics and other smuggling routes. In this category, all imaginable manner of exotic methods become theoretically possible.

Border monitoring solutions must address the full range of options for entry. In addressing the possibility of border violations, we need to consider all three of these modes—among migrants along migrant routes, with criminal assistance and use of routes established by criminal organizations, and utilizing tactics devised, tested, and executed wholly within a terrorist network.

Since one means of entry through illegal channels is to mingle in the flow of migrants and seasonal workers, finding an effective way to reduce the flow of unauthorized migrants is important for reducing opportunities for terrorists. The current system of border and immigration management rests on a political bargain that has satisfied most citizens for decades—strong legal prohibitions on immigration to satisfy the views of those who would limit immigration for social or budgetary reasons, but low enforcement to satisfy employers and those who support maximum economic growth. This bargain has become decidedly less persuasive on security grounds. At least half a million people enter the United States illegally each year, mostly to work and join family members—a flow exploited by hundreds of criminal gangs for whom the line between being paid and violent victimization is easily transgressed.⁴² From a counterterrorism perspective, this represents the worst circumstance—a large population that has entered and continues to enter through illegal channels and remains dependent on and therefore perpetuates an illicit infrastructure; ineffective enforcement of immigration laws; and strong prohibitions on immigration or even on stays for seasonal work that fuel more illegal stays and criminal support. Beyond the direct security impact, there is also an unseemly

national hypocrisy to such blatantly contradictory policies that undermines the legitimacy of our legal and political system.

The counterterrorism perspective adds only one angle to the immigration debate—an urgent impetus to arriving at a solution that actually *works* in practice. The ongoing attempt to amend the current immigration bargain simply by increased enforcement—building up physical barriers, detection measures, and border patrol, especially at the Southwest border, with more severe legal consequences for immigration violations—seems doomed to fail as a practical matter.

The ineffectiveness of enforcement-based measures to stop supply where there is demand is the glaring lesson from multibillion dollar strategies to stop illegal drugs from coming into the country by attacking the growers, traffickers, and smugglers—attempts that have had only a limited impact beyond shifting supply from one set of sources and routes to another. Until we make a serious effort to reduce demand for heroin and cocaine, suppliers will continue to defeat enforcement efforts, relying in part on their ability to corrupt officials throughout the system. But while thus far we have gotten away with treating dangerous drug use largely as an exercise of individual liberty—a so-called victimless crime that does the most damage to its user, and therefore a problem for which an ineffective solution is politically acceptable—this will *not* even arguably be the case where terrorism is at issue, as it is with immigration policy.

In the immigration context, the enforcement solution seems as unlikely to be effective as it has in dealing with the narcotics trade—there is a strong demand for workers from the US economy and a deep desire for migration by people pursuing opportunity and family unification. Even a fairly applied regulatory or criminal enforcement system will be overwhelmed unless there is a large measure of voluntary compliance by people who see the laws as fair and workable. And we cannot raise the level of force substantially; human rights considerations—and simple human decency—do not permit us to treat migrants as if they are violent criminals or terrorists. If we were to ignore these considerations and raise the level of force—in effect attempt to militarize our borders and build a Maginot line—we would both be ineffective and quickly forfeit

the cooperation of the Mexican government and people, who are critical to developing information about terrorists potentially attempting to transit the country.

Market forces must be enlisted to shrink the illegal market for labor so that there is less pressure on US enforcement resources and we can build up a partnership with the government and people of Mexico in controlling crime and in counterterrorism. It is therefore an urgent matter to revise the terms of the historic immigration bargain—to raise the level of permitted immigration somewhat to satisfy economic demand or accept a reduction in economic growth—while strengthening incentives to adhere to the rules. Incentives may be economic, regulatory, or criminal. How much the level is raised, whether the grounds for permissible immigration are narrowed, and how to structure incentives and enforcement for immigration purposes, are beyond the scope of this discussion; these factors depend on careful analysis of market, social, and human rights factors that are for the most part independent of immediate terrorist mobility countermeasures.

The role the military and military tactics should play in perimeter control is emerging as a significant question. Our first instinct may be to turn to the military to assist with perimeter control and the military may have its own impetus in that direction. After 9/11, some governors sought assistance from military personnel to provide a combination of practical assistance and public reassurance at airports and ports. This led to a further development of concepts of military support in relation to terrorist attacks, particularly for emergency preparedness and response, but also as somewhat ambiguous “support” for civilian border authorities. At its own initiative and seeking to define its own role in homeland defense against terrorists, the military has recognized a greater need for domestic “force protection.” To protect its own forces, it has become more involved in the problem of cross-border movement of people, has established a new Northern Command, and is building on the military’s involvement in counternarcotics operations in the Southern Command. Additionally, Congress, has required DHS and the Department of Defense to come up with a joint plan for border defense to counter migration through illegal channels from Mexico. Thus, there is both precedent and momentum for some form of military involvement in border-related counterterrorism.

An additional, reinforcing factor is a practical and historical one—monitoring our borders is a large-scale problem in the sense of requiring complex planning and major installations of sophisticated technology. We associate planning and technology investments on this scale and of this type with the military and the military-industrial support complex built up during the Cold War.

But there are important reasons not to defer reflexively to military authority and expertise. First, the military is not organized to defend US borders. Defense of our land borders has not figured prominently in national security strategy in recent history because we have fought our enemies overseas. Second, the legal principles of *posse cometatus* expresses our national conviction and constitutional law that civilian, not military, authorities should police civil society. Already there has been some friction between DHS and DOD, including between the Coast Guard and Navy in defining protective requirements in the maritime border context and surrounding intelligence activities and integration. Ultimately, the prospect of monitoring for terrorist movement over our perimeter requires us to work out answers to very basic questions: to what extent should surreptitious entries by unknown individuals and small groups (who are not known to be members of military forces) across border points be dealt with as issues of invasion or sabotage, as matters of counterintelligence, as immigration law or as domestic law enforcement responsibilities, to be handled by military, intelligence, immigration law, or domestic law enforcement principles, authorities, processes, and tools? Answering these questions is as much a matter of deciding what is feasible and effective as deciding what is constitutional and legitimate.

Border monitoring is sufficiently challenging that it cannot be handled solely by the federal government; local communities and neighboring governments and their citizens must be involved. Successful long-term immigration system reform and a growing standard of living in Mexico may help in the achievement of a more orderly border with Mexico and diminished use of those channels. Reducing risks of terrorist association with narco-traffickers and other smugglers will be a continuing challenge. But even reasonably successful immigration reform and crime control will not fully address the problem of terrorist entry through illegal channels. The potential will remain

for clandestine infiltration across borders well away from the major illegal channels used by migrants and smugglers.

Defending frontiers seems like a fundamental responsibility of sovereign governments, but to defend against infiltration by a handful of extremely dangerous individuals is quite different from monitoring for approaches and incursions of known military forces, even in small parties of saboteurs. A nearly limitless number of entry routes are offered by our maritime, land, and air space borders, something well known to law enforcement authorities dealing with the smuggling of drugs, arms, and cigarettes among other commodities. The technical and intelligence methods developed in the context of the Cold War are based on the movements of military forces significantly more visible than these small but dangerous groups. Since the problem of finding terrorists is not fundamentally a military problem in the traditional sense, it does not have a military solution.

Clearly, counterterrorism is also different from the task of enforcing immigration laws. Should the United States prove able to use immigration law reform to reduce the overall number of migrants and seasonal workers entering through illegal channels—from Mexico primarily, but also from Canada and coastal entry points—we will continue to require monitoring of known migration routes and the terrorist threat will remain along the thousands of miles of land, river, and sea borders that over time can be studied, probed, and crossed clandestinely. Already a separate maritime strategy to address terrorist mobility by sea is being developed.

Whatever we design to reduce our vulnerability to this threat will involve some form of monitoring and response capability supported by integrated intelligence. To carry out such a complex program across so much space and so many jurisdictions, we need all the help we can get. It is simply a fact of life that local authorities and people living in border communities and remote locations can be helpful in spotting potential trouble and in responding to intelligence alerts. To advocate citizen alertness, local, regional, state and cross-border planning with processes for communicating with federal counterterrorism authorities, is not to promote vigilantism. Vigilantism that creates a climate of persecution is a form of injustice and will alienate people who might oth-

erwise volunteer or be willing to alert authorities to terrorists and violent criminals.

To build up joint efforts with our neighbors along shared perimeters, we must invoke mutual interests to achieve more effective security. Canada is also a target for Al Qaeda and we can at least base a diplomatic program on the assumption that no sovereign authority wants unscreened entrants. We also need to respond to concerns of those from whom we are seeking assistance.

Since perimeter control can never be absolute, any more than screening systems can be perfect or crime control methods fully effective, we have to recognize the importance of indirect systems of reducing vulnerability. Joint efforts with Canada and Mexico to strengthen the North American perimeter against illegal entry through both legal and illegal channels are therefore important strategic elements of US perimeter security.

Constraining terrorist movements requires the United States and its allies to provide assistance and training in frontier defense for security partners whose territories are targeted by terrorist organizations as locations for sanctuary and transit. Beyond the North American perimeter, a terrorist mobility strategy requires systematic attention to the borders of state sponsors of terrorism, key terrorist transit regions, and assistance to foreign governments in border defense force training where there are vulnerabilities to terrorist incursions for safe havens among other activities. Key among current focal points are the borders between Syria and Iraq, between Afghanistan and Pakistan, and transit routes to Europe from South Asia, and Africa to the Middle East.

Setting risk management priorities for domestic and foreign border-monitoring activities is an important aspect of a terrorist mobility strategy. In view of the wide range of possibilities for entry through breaches of frontiers, long-, medium-, and short-term priorities are essential. On one level they depend on a broader counterterrorism strategy. A basic principle, however, is that we cannot afford to ignore any dimension of this problem. Priorities and resources for countering terrorist mobility must focus on a full range of possibilities—US

borders already subject to high levels of surreptitious border crossings; remote but still accessible US frontier border areas; the North American perimeter and the Caribbean region; and the key terrorist transit and sanctuary zones around the world.

Is DHS's goal of achieving operational security of both the northern and southern borders within five years realistic and achievable? From a terrorist mobility perspective, the goal is certainly important, but in deciding how to pursue it, we must keep in mind the proximate threat, as well as of our range of vulnerabilities, and what is likely to actually work. This requires much more detailed planning and thought than is evident from public declarations.

The current priority for Congress is preventing migration from Mexico through illegal channels, which tends to result in resources being concentrated along the US border with Mexico. The ways in which our concern with migration differs from our concern with terrorism, however, must be kept in mind.

Suppose for the moment that there is a greater threat from senior level "deep cover" operatives enjoying legally issued Visa Waiver Program passports than from Mexican border entries by "mules," a greater threat from entries across the Canadian border by "mules" or even higher level operatives than from Mexican border entries, and a comparable concern from individuals already resident in the United States. *If* this is so, building up remote border capacities, while an important ongoing agenda item, is not as important as significantly raising the standard of constraining terrorist mobility through legal channels, while also raising the level of attention to human smugglers and organizations facilitating other clandestine travel.

To make decisions about priorities in countering terrorist mobility, we need to know which neighboring country is the source of more travelers who generate watchlist hits, and where more known terrorists reside. Answers to these questions are likely to compel the conclusion that our border with Canada is a more immediate concern. Certainly, Islamist terrorists may migrate to Mexico to attempt entry among other non-Mexican migrants. But Canada is a nation with a

history of Islamist terrorist presence and with Muslim communities in Montreal and Toronto, cities close to the border that are vulnerable to exploitation by terrorists seeking cover.⁴³ In the rush to fortify the southern border and increase enforcement resources—a strategy that has not served us well until now and promises to be no more effective in the future—we should not overlook the actual risks posed by terrorist mobility.

All-encompassing terms like “border security” make optimal risk assessments relating to terrorism more difficult. We must be honest about the difference between terrorist mobility as a threat and other vital security issues at stake in border control—violation of immigration laws, criminal activity with national security implications (e.g., smuggling of weapons of mass destruction, or biological or chemical weapons), and public health protection. Without a degree of refinement in our thinking, we will find ourselves making choices with our security dollars that we will regret in the future.

G. Domestic Security: Constraining Terrorist Mobility in the United States

Actions outside the United States and at our borders cannot entirely prevent terrorist attacks here. We face a continuing risk that terrorists will successfully enter the country and embed themselves while they plan and execute operations, or will emerge from within our population. Once here, terrorists use governmental and private sector systems to move around including the immigration system with its regulation of employers, which confers legal status and verifies identity, and the public and private transportation systems. We do not yet have a domestic counter-*mobility* strategy as such to protect against or exploit terrorist use of those systems. The discussion here is limited to the immigration system.

The lack of a domestic terrorist mobility strategy is especially troubling because it seems likely that the gap will be difficult to close within the current organization of counterterrorism. Why there is a no proactive policy to focus on *terrorist* exploitation of the immigration system within the United States seems as intractable as it is obvious. The FBI has been designated the exclusive domestic counterterrorism agency, but the

policy-level officials, and most of the thousands of working-level officers who are experts in the methods that terrorists use to embed themselves in foreign countries, and in the the complex laws, regulations, and procedures that govern immigration, are overwhelmingly located in the Department of Homeland Security and the Department of State. (Exceptions are the rump immigration administrative law court that remains in the Department of Justice—DOJ), and the DOJ criminal attorneys who supervise human smuggling and trafficking cases.) There are of course cases involving terrorist mobility tactics being made by FBI-run Joint Terrorism Task Forces. But field investigations are not the same thing as a meeting of the minds at the senior policy levels. Until very recently, there was no senior policy level at the Department of Homeland Security in position to design such a strategy.

The gap in the policy arena of domestic terrorist mobility is hard to exaggerate. At one point in 2004, ICE testified to Congress that its highest priority was attacking internet pornography—no mention of counter-terrorist embedding. One can go too far, however, in concerns about policy and strategies. The lack of an integrated policy to use regulatory and enforcement resources relating to immigration to detect, exploit, and deter terrorist movements does not mean that nothing is happening. Significant efforts have been made within the limitations imposed by the legal and organizational structures. First, there are prosecutions and legislative and sentencing changes focused on domestic illicit travel networks. Other programs distinct from general immigration enforcement include:

- Improved terrorism-related screening in immigration benefit processes;
- Increased detentions of “other than Mexicans” (OTMs) who enter the United States through illegal channels;
- Increased immigration law enforcement attention to workers at critical infrastructure sites; and
- Prosecutions of individual terrorism suspects that make use of immigration law and related identification fraud charges frequently used in lieu of or to supplement terrorism-related charges.

In addition, pending legislation would increase resources for interior immigration enforcement and impose new compliance requirements on

employers, which would expand the platform for, but in no way guarantee, meaningful efforts to find terrorists.

Although there are at least these activities, and likely more, they are not the best we can do. A deliberately developed domestic terrorist mobility strategy would optimize the vulnerability exposed by terrorists' need to function in the United States under false pretenses, and focus attention on potential terrorists rather than migrants generally.

A fundamental first step is to adopt specific goals related not to general immigration enforcement, but to diminishing the likelihood of terrorist attacks. Three important goals are: (1) using immigration violation indicators (including reference to travel document and supporting identification) as an active defense to identify terrorists who were able to enter undetected through illegal or legal entry channels, and a parallel effort ensuring through intelligence, enforcement, and regulation that such terrorists do not embed themselves by obtaining or maintaining legal immigration status; (2) establishing reception and integration policies that minimize the possibility of Islamist terrorist commitments being adopted by visitors, immigrants, or citizens; and (3) reducing vulnerability by establishing the principle and reality of reliable identification of individuals, including US and non-US citizens present here. These three goals are not intended to exclude the critical tactical threat warning and other preventive action already emphasized in the *National Strategy for Homeland Security*, and the build-up of protective measures at critical infrastructure facilities. Adequate credentialing and identification systems are indeed aspects of critical infrastructure protection.

In support of these goals, to be pursued at all levels of government and through the private sector, four areas of activity are central to an integrated domestic terrorist mobility agenda:

- Terrorism-specific immigration law compliance and enforcement policy;
- Screening architecture that permits domestic, border, and foreign systems to be compatible;
- Knowledge of our own population and responsible treatment of immigrants; and
- Reliable identification for all people in the United States.

The following discussion of these arenas aims to demonstrate a mode of thinking about how to integrate and optimize efforts against a particular and important terrorist vulnerability. Other policies and programs than those described here may be as or more important.

1. Terrorism-specific immigration law compliance and enforcement policy

Deft use of immigration law must be a pillar of domestic efforts to deter, detect, and disrupt terrorists in the United States. But discussions of immigration law-related domestic counterterrorism tend to conflate general law enforcement programs aimed at any migrants with illegal status with tactics specifically aimed at terrorists. On the other hand, law enforcement programs to find terrorist individuals, organizations, or cells do not have a well defined mobility component.⁴⁴

The general immigration civil compliance and criminal enforcement measures linked to terrorism in recent policy discussions include: increased use of detention; expansion of expedited removal; worksite enforcement; employer sanctions; limits on access to transportation through restrictions on drivers' licenses; and expansion of enforcement resources through mandates for state and local agencies. Such programs are too broadly focused to be relied upon as counterterrorism measures. To constrain terrorist mobility and take advantage of the vulnerability created by the need to remain mobile, there must be a more targeted set of tactics that are clearly defined and well funded. Several examples come to mind.

- **Rigorous screening processes for US passports.** A US passport is a desirable tool for any clandestine traveler, so US passport offices should have a document screening program that detects problematic identification documents. Among other critical roles, a central data collection and analysis unit for all the passport offices should be a bellweather for the security of the US birth certificate system. Additionally, fingerprints should be part of US passports, unless equal security is achievable through other means.
- **Stringent security screening of applicants for immigration benefits.** There has to be a rigorous security screening process for

applicants for immigration benefits. There may be errors in the initial visa and entry process (or entry through illegal channels), documents may be altered between entry and application for benefits, and new information, capabilities, or circumstances may arise between entry and application for benefits. In addition, as discussed in Subsection C (Attacking the Illicit Market), problems discovered in immigration benefit screening provide a critical opportunity to trace the fraud or other problem back to its source, leading to criminal cases or intelligence-gathering operations.

Three elements of immigration benefit security screening are critical. First, there must be a high-level capacity to scrutinize travel documents for terrorist links as a supplement to biographic and biometric watchlist checks. It must be informed by the same intelligence methods that are needed at the consular and port of entry checkpoints. This would both raise the level of fraud detection and enable officials to discover document indicators associated with terrorist groups. At least some of this capacity can be electronic, beginning with document authentication.

Second, there should be a single electronic file for non-citizens admitted to the United States accessible throughout the system, from visa through naturalization and passport issuance. Such a file is essential for providing complete and accurate information and for avoiding time and resource-wasting redundancy. This is an announced goal of the US-VISIT program.

Third, immigration benefit screening must be supported with a well funded central information unit for the acquisition, integration, and analysis of data from US field offices. This unit should have its own intelligence capacity, and be a source of case referrals to benefit and enforcement field offices, and provide strategic analysis and reporting (including to relevant Congressional committees). Data from cases with terrorist links can be accumulated and analyzed to show practices against which new steps have to be taken. The unit must address what many in the immigration community know anecdotally, but what is disputed at the policy level because facts are not available—the scale of precise types of fraud in the immigration benefit system—so that

resources can be focused on reducing priority vulnerabilities through needed law enforcement, legislative, regulatory, or process improvements. The information unit should be linked to, and accessible by, the broader intelligence and law enforcement communities, with appropriate privacy and case coordination safeguards and procedures.

- **Visa overstay and student visa terrorism surveillance programs.** As with immigration benefit screening, immigration benefit enforcement within the United States should have specific counterterrorism programs. ICE has specific programs targeting pornography, money laundering, and terrorist financing that link compliance, enforcement, and regulation, but no specific terrorist mobility programs distinct from general immigration enforcement. This is a policy, organizational, and operational challenge that can and must be met.

For example, a dedicated terrorist mobility unit at ICE (joined by temporary duty consular officers) should be looking for potential terrorists among visa overstays. The unit should systematically compile and review visa overstay information against terrorist watchlists and other available government databases, setting priorities according to terrorism-based criteria. For instance, Visa Waiver Program countries are a logical priority. Although the United States does not yet have comprehensive exit controls—these are mandated and incorporated into planning for US-VISIT—we do have some exit information. This unit should be supported with automated analyses and reporting that highlights cases of potential interest to field offices and policy officials.

A similar unit should be dedicated to routinely and systematically reviewing potential student visa violations using terrorist watchlists and other available government databases. Shifts in education plans to subjects that implicate national security must be tracked and followed up by at least the same checks that would have been conducted had the student initially applied to enter on a visa that permitted this course of study.

Such visa overstay and student overstay surveillance programs complement counterterrorism case investigations by Joint Terrorism Task Forces (JTTFs), which typically investigate

immigration status information for particular suspects on a case-by-case basis. JTTF case information about visa practices should be provided to the central terrorist mobility data units at ICE in real time, in order to inform its screening and ongoing investigative analysis, for which the JTTFs in turn are among the most important potential recipients.

- **State and local authority participation in a national terrorist mobility strategy.** State and local authorities must be included in an organized way in national efforts to counter terrorist mobility. The major day-to-day tool available to the full range of state and local authorities for contributing to national counterterrorism efforts is the connection to the Terrorist Screening Center (TSC). Officials query the TSC for biographic information about individuals they suspect may have a connection to terrorism, or simply want to check in a routine way at a traffic stop. The query results in information being transmitted to federal authorities while local officials receive guidance on appropriate handling of the individual.

In addition to obtaining biographic information and/or guidance, state and local authorities must have a routine system through which they transmit electronic images of an individual's travel and supporting identification documents to a central terrorist mobility documents unit (proposed as a new DHS component in Section IV) for terrorist indicator screening. Responses with information and guidance would go back to local and federal counterterrorism and immigration authorities with data preserved, disseminated, and analyzed centrally. In addition to this type of routine interaction, state and local authorities in high-immigrant population locales are in a position to observe anomalies, like repeated exploitation of certain visa categories. A framework for local, state, and federal interaction must be built on such insights. Training state and local authorities in document analysis is a requirement, with a system for rotating state and local travel and identification document specialists through relevant federal agencies and for rotating federal specialists through state and local agencies. Arrangements at the state and local level should be further defined by the states and localities through the homeland security planning processes.⁴⁵

General police information practices, like systematic routine fingerprinting of arrestees, would provide an opportunity for real-time checking against other biometric databases, including terrorist biometric databases. (As discussed in Subsection E, state and local authorities also need to play a partnership role with federal authorities in unravelling any local illicit travel infrastructure.⁴⁶)

- **Critical infrastructure worksite enforcement.** Immigration and Customs Enforcement should have a distinct terrorist mobility program. Today's major counterterrorism program is the critical infrastructure worksite enforcement program, an indirect measure that cannot substitute for efforts specifically aimed at detection of terrorists. The difference between an indirect and direct measure is significant.

ICE's critical infrastructure worksite program checks the immigration status of employees at workplaces that DHS deems to be critical infrastructure, and takes follow-up enforcement action against the migrants themselves, though not necessarily the employers. There is a rationale for this program. Terrorist threat assessments tell us that Al Qaeda's goal is to carry out attacks that will kill as many people as possible, cause a reverberating economic impact, and have a larger social and psychological impact that can reshape national politics. Since critical infrastructure facilities offer targets that clearly meet these goals, they are particularly vulnerable, and the reliability of the workforces in these facilities is particularly important.

This type of worksite immigration enforcement is neither general immigration enforcement—such as apprehensions at the Mexican border—nor directly terrorism-related—like adding a TSC check to the checks done at traffic stops—but rather a security measure that is in between and indirect. It inevitably communicates the assumption that foreign nationals as a class necessarily pose a danger to national security, and for this reason alone is a blunt instrument. For critical infrastructure protection, what matters is not the nationality of a worker per se, but whether that worker meets the security level appropriate for the work being performed. Since we welcome foreigners into the US military and many scientific and medical institutions,

there is no reason why foreign nationals should not work at critical infrastructure facilities—unless it would constitute a national security risk. What can be said for this program is that when workers at such facilities do not have legal immigration status, they are potentially subject to pressure by others, which creates a degree of risk. Vulnerable immigrants are not the only groups among which terrorists can recruit, but information or help from workers is one means of gaining access. Therefore, absent federally approved credentialing and screening programs for critical infrastructure, and a program for securing employer compliance with these laws, it seems prudent from a security perspective for unscreened non-citizens without legal status to be removed from their jobs at facilities considered at particular risk for terrorism.

When a worker is removed on immigration status grounds from the critical infrastructure facility—and the employer is fined or otherwise penalized—the security vulnerability is eliminated, unless the individual is actually suspected to be a terrorist or criminal. There may not be any discretion in choosing to continue the immigration case, but whether an immigration case against the individual should be pursued ought to depend on the overall priorities and resources of the immigration enforcement system, including its resources being dedicated to terrorist mobility programs. (It seems probable that most migrant workers would seek new a position less likely to be targeted.) While there will always be a need for critical infrastructure employer auditing, just as there may be for tax or other regulatory purposes, the current program cannot be viewed as a long-term substitute for a strong system of adequate screening and credentialing backed up by management certification for critical infrastructure employment. This would be much more cost-effective than attempting to cover the range of workplaces and would permit enforcement resources to be preserved for terrorists, violent and organized criminals, and other priority cases.

- **Security policy toward the estimated 10 million resident migrants without legal status.** Not only at critical infrastructure worksites, but generally, enforcement priorities toward the 10 million foreign nationals residing here in illegal or quasi-legal immigration

status pose problems of prioritization from a security perspective. The primary terrorism threat our border authorities face today is from Islamist terrorists. Most of the 10 million unauthorized immigrants are Mexicans or Central Americans who came to work and/or join extended families. This tells us that *the vast majority* of immigrants living here without legal immigration status are highly unlikely to pose a terrorist risk. Whatever views people may hold about immigrants' access to welfare and jobs, roles in crime and disease, and impacts on our culture and society, the concerns or threats that may exist on those grounds do not rise to the level of across-the-board *terrorist* risks. For this reason, a policy of deporting everyone who entered or remained illegally on the grounds that a few might be terrorists would be at a minimum grossly inefficient counterterrorism.

An argument for such a program is that there would be an incremental bonus security benefit from an all-out enforcement program. But even the most draconian of plans to remove people depend on the idea that there will be some voluntary compliance, and a terrorist who is successfully embedded here is unlikely to comply. Moreover, there is a political and counterterrorism cost to such a sweeping approach. One may agree or disagree that an expulsion policy would be inhumane, but if the political consequences internationally for the United States of expelling or inciting the departure of 10 million mostly hardworking, decent people were objectively assessed, the assessment is unlikely to be positive. Our "public diplomacy" does not need this additional handicap, nor would Mexican internal politics and our relationship with Mexico—crucial for maintaining effective programs to constrain terrorist mobility—benefit from this additional incitement. And since migrants from poor countries often send back remittances, we would have to ask whether the economic and social consequences would be counterproductive, given our goals of promoting economic development and expanding world trade states as means of reducing the impetus for immigration outside of legal channels and for reducing the economic and social conditions that give rise to terrorism.

Nevertheless, while it would be disproportionate and counterproductive to attempt mass deportation, it is unacceptable to persevere in a

system that allows so many people to live and work here who have not met at all, or only partially met, screening requirements for security purposes, among whom there could be some highly dangerous individuals. The line between assigning immigration enforcement resources to critical infrastructure facilities but not major shopping centers or construction sites is ultimately a thin one. Shopping centers are also attractive terrorist targets and the retail sector that would suffer ripple effects from an attack is critical economic infrastructure. As has been discussed, workers vulnerable to pressure by terrorists represent a greater degree of risk than those who are not, and the illicit market in travel and identity documents generated by the unauthorized population in the United States is a resource for terrorists. Even though we do not face a grave threat from the population as a whole, it should be an objective to bring as many individuals as possible into legal channels as soon as possible. As a state governed by just and fairly enforced immigration laws, our persuasiveness in global fora would be enhanced, as well.

- **Immigration charges and terrorism suspects.** Terrorist exploitation of immigration and transportation systems is a valuable focus for counterterrorism, just as is terrorist misuse of financial and communications systems. Contact with these essential systems requires terrorists to conceal their identities and agendas, and their evasive measures in turn make terrorists vulnerable to detection. From a tactical perspective, therefore, immigration law-related audits or investigations are an important proactive tool in the search for terrorists and terrorist organization infrastructure.

Terrorism-related immigration law civil and criminal investigations potentially serve multiple purposes. A fraudulent travel document with terrorist indicators caught by a border inspector may disclose a dangerous individual in the first instance, confirm a terrorist identity, and/or enable officials to trace the document back to a source which can then be the subject of further law enforcement or intelligence action. In fact, debriefings of *all* terrorist suspects regarding their mobility tactics should be standard practice, with the information made available in real time in a standard format to all relevant analytic units dealing with terrorism.

A powerful investigative package begins to be assembled when immigration-related techniques are combined with those of investigative and regulatory authorities relating to terrorists' need for surreptitious financial support and internal and external communications. Treating terrorist mobility as a discrete subject matter, as this report has done, underemphasizes the practicalities of its use by investigators and intelligence officers as one of many counterterrorism methods.

But prosecutors' use of immigration charges in lieu of terrorism charges does raise some questions. Charging terrorists with criminal immigration offenses appears to be a frequent path of choice for prosecutors, the salient advantage being that government must rarely disclose sensitive or classified information in order to charge the individual, yet any terrorist activity can still be disrupted. This can be important where there is solid evidence that the suspect is a terrorist. But under these circumstances, fairness in the enforcement attention given to groups by national and religious origin and standards of due process are particularly vulnerable. There is no internal or external reporting that would permit assessment of miscarriages of justice and infringement of civil liberties and human rights that may have occurred in immigration investigations linked to terrorism cases. Some form of accountability for short- and long-term results should be required. Otherwise mistakes that are too frequent and require official explanation, apology, or compensation can lead to the needless alienation of members of population groups—Muslims or Arabs today—who should be a source of support and information, and *who instead may transmit a negative view of American justice to their nations of origin, where a sense of United States government injustice fuels the attraction of radical Islamic ideology.* The risks not only of injustice, but also of undermining constitutional legitimacy, and fueling enemy fires must be taken into account in domestic enforcement policymaking.

A number of commentators have observed the negative impact of mistaken prosecutions in engendering resentment and fear among Muslims and in stoking fears of Muslims among the rest of the population, and concluding that the “legal war on terror” so far, to the extent that it can be assessed by the public, has not been an

effective counterterrorism tool.⁴⁷ Where justice is concerned, even the perception of ineffectiveness requires the United States to take a closer look and improve what we are doing.

2. Screening architecture that enables compatible domestic, border, and foreign systems

There must be compatible standards for identification, credentials, and screening in order for officials at the various stages of processing of visitors and immigrants, and of critical infrastructure and transportation access, to benefit from the information developed at other points in the system. For this reason, it is important to establish the planned DHS Screening Coordination Office as a critical node in the process of setting standards for, reviewing, and linking the various systems for screening. Working closely with other DHS offices—for US-VISIT, for policy, for privacy and civil liberties—the Screening Coordination Office has a major role to play in helping establish compatible biometric standards, eliminating stove-piped systems, working on data integration, formulating policies for credentialing and identification, and helping to reduce the error and delay rates in the use of these systems. In setting priorities among the myriad tasks, there must be a distinct focus on establishing the optimal conditions and systems to detect terrorists, curtail terrorist mobility and deny terrorist access, without assuming that terrorists are noncitizens.

3. Knowledge of our own population and responsible treatment of immigrants

Knowledge about immigrant communities and their cultural heritages is essential for informing operational counterterrorism and for developing policies that support successful integration of immigrants and visitors into US society. A missing piece of the new counterterrorism environment is the governmental assignment of responsibility for assessments of domestic communities in relation to terrorism. Such assessments must draw upon academic and other outside resources, but they are sufficiently important to national security to be designated the responsibility of a government office.⁴⁸ The studies would stay abreast of the potential for terrorist (or criminal group) emergence and sanctuary and thereby provide context for individual cases and support DHS's development of visitor, naturalization, and enforcement policies.

The gap likely results in part from the foreign-domestic divide and in part from the lack of importance assigned to analytical practices by most domestic law enforcement organizations. The NCTC and CIA are clearly responsible for the preparation of in-depth analyses anticipating or describing the emergence and organization of terrorist groups in *foreign nations*. The FBI is clearly responsible for preparation of analyses of *actual suspects or tactical, domestic threats*, such as known terrorist organizations. Both of these tasks potentially spill over into background discussions relating to attitudes and circumstances in domestic communities. Such studies need not exceed legal boundaries but they risk giving rise to complaints about singling out a group for intrusive or punitive investigation. The distinction between investigation and analysis has to be clear and we must address the anomaly that we likely have more strategic analytic resources for understanding communities in foreign countries than in our own.

Without waiting for in-depth insights, we can safely assume that student visitors do not necessarily know our laws and cultural mores. Consideration should be given to preparing informational pamphlets for incoming foreign students providing guidance on hate speech, terrorism crimes, violent crimes, and freedom of religion and expression. This is a precaution against students running afoul of unfamiliar customs and laws, for instance rules about participation in demonstrations without permits or in advocating particular acts.

4. Reliable identification for people in the United States

Secure identification is a topic at the center of preventing and disrupting clandestine mobility because without it, biographic data checks are useless. With respect to individuals born in the United States, a necessary foundation for reliable identification is the security of US birth certificates and the process by which they are issued. Birth certificates are “breeder” or “feeder” documents that enable individuals to acquire passports, driver’s licenses, and other credentials. As long as the birth certificate system is weak, the weakness will be transmitted to any identification system that relies on it. Legislation has mandated reform of the sprawling system of birth certificate issuance, and a regulatory process is underway. Once there is such a system, or even a decision on the design of such a system, it makes sense to assess where we are and decide what additional documentation a birth certificate should be used to support.

With respect to naturalized citizens and foreign visitors, we must look to passports, foreign birth certificates, and corroborating documentation and information of various kinds, making travel and identification document security a priority for terrorist mobility diplomacy worldwide.

Actions within the United States remain constitutionally and practically distinct from actions against foreign citizens overseas and immigration-related security measures at our air, land, and sea borders, and therefore a distinct, domestic terrorist mobility strategy is important. But a strictly US-focused approach is also fraught with a number of potential pitfalls. As with many aspects of counterterrorism, one difficulty is in the complexity of all the multiple outward and inward linkages necessary to deal with the domestic component of a global phenomenon.

Terrorists operate along a mobility continuum, exploiting in turn global travel routes, borders, immigration status within a country, and domestic transportation. During each stage of movement, terrorists are potentially exposed to detection. If parochialism triumphs and domestic counterterrorism is designed without regard to these linkages, critical information will be lost and costs will be higher. For instance, unless internal countermeasures are coordinated with border controls, the United States will end up paying for a multiplicity of incompatible identification, biometric, and credentialing systems. This would deprive us of necessary information linkages enabling us to detect dangerous individuals who successfully exploit one or another component.

Lack of imagination and expertise in the spectrum of potential relationships among immigrants and citizens, and citizens and foreigners, here or abroad is another potential pitfall. The Islamist terrorist movement is subject to emergence, at least on a small scale, nearly anywhere. Although the major risk for now appears to be from foreign citizens, US citizens may take up Islamist terrorism, as illustrated by the case of suspected Al Qaeda trainee Jose Padilla, among a few others. Further enlistment and recruitment of US citizens seems almost inevitable.

Too much reliance on a domestic approach, however, places us at risk that we will fail to see and act against the larger patterns of terrorist movements globally, and in the event of imminent attacks, fail to

“connect the dots” that would alert us to particular threats. Terrorist recruits in the United States may include prisoners exposed to violent ideology or home-grown violent extremists. These home-grown extremists may seek assistance from other groups. Terry Nichols, a pro-gun, antigovernment ideologue is serving a life sentence for his role in the April 19, 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City. It appears certain that Nichols obtained training in bomb-making from members of the Abu Sayyaf Brigade while on a trip to the Philippines.⁴⁹ The Nichols case is a vivid illustration of the importance of using any counterterrorism tools in the context of a broader counterterrorism agenda, supported by a common screening and intelligence architecture, and under centralized coordinating management.

H. Recovery: Post-incident Terrorist Mobility Reviews

A terrorist mobility policy needs to be intelligently dynamic; it must evolve over time based on new knowledge. Among the more fertile opportunities for acquiring that knowledge are systems that fail—when terrorists are found after the fact to have entered the country, when they gain access to a target facility, or when they enter and carry out any attack before being detected.

It has already been suggested above that the NCTC or DHS should compile information about all attempted but detected incidents of terrorist entry or domestic embedding on an ongoing basis in order to discern trends and practices in border and immigration incursions and countermeasures. Establishing such reporting is a not unfamiliar challenge for government agencies. But post-terrorist attack reviews are even more sensitive than compilations of information about entry or post-entry encounters, because of the scale of failure involved. And because reaction to the attack can aggravate the damage already caused, it behooves us to engage in planning not only for first-response to victims and restoring infrastructure, but for restoring public confidence.

As has been so memorably phrased by Steven Flynn, in the United States after 9/11, we boycotted our own country by shutting down our system of air travel and slowing cross-border traffic nearly to a halt.⁵⁰ Somewhat later, military personnel were stationed at the airports and

border ports of entry, in part to provide reassurance and promote confidence that would encourage people to resume travel. Depending on the circumstances, the costs of closing ports of entry may be supportable—for instance, for purposes of a quarantine. But the next time we suffer a terrorist attack, we should be positioned immediately to launch an in-depth examination of the vulnerabilities of the travel, transportation, border, and immigration systems that contributed to the terrorists' success as one element of the process of rapid recovery.

Review bodies and procedures exist in various forms—Inspectors General, the Government Accountability Office, the National Transportation Safety Board, post-battle or incident military reviews, and new proposals aimed at reducing medical errors. Designing a special body or process for analyzing terrorist homeland entry incidents seems warranted by the complexity of the systems involved, and the volatility of the politics surrounding immigration and border control. Airline accidents are investigated by experts from the nations of the crash, the airline manufacturer, and the airline. A similar multinational team might be called upon to review mobility factors relating to a terrorist incident.

One aspect of preparedness, then, should be an analytic review team to prepare a comprehensive terrorist entry and immigration assessment report under the auspices of the National Counterterrorism Center and the Department of Homeland Security. The imperative is for the government to close exploited loopholes and improve security as quickly and publicly as possible to restore public confidence and willingness to use the affected systems.

IV. DIRECTION, MANAGEMENT, AND ORGANIZATION OF A TERRORIST MOBILITY STRATEGY

Strengthening performance across the range of efforts against terrorist mobility requires dismantling institutional barriers that have evolved

from historical divides and organizational cultures. In approaching this challenge, it helps to understand that the border and immigration arena is a distinct legal and practical terrain. This is easy to miss because our strategic thinking has evolved from a view of the world that sees us as one state facing other states, to also facing a meaningful threat from participants in stateless organizations and networks like Al Qaeda, and to a lesser extent against transnational criminal organizations without political agendas but which might be involved at the margins of terrorism.

In keeping with the new threat, thinking about warfare and crime control has expanded to include tactics against organizations using terrorism and linked criminal support networks, and to solving problems associated with the new tactics—especially ensuring that we maintain continuity between our efforts overseas and our efforts within the United States in order to “connect the dots” operationally.

We have not yet solved the problems arising from the foreign-domestic divide in our national security strategy. But as we wrestle with this problem, what warrants more thought in the emerging security framework is the concept that between and among nations and their enemies is a third zone: the border and immigration arena and its supporting transnational transportation networks. In this zone, people (and goods) are subject to particular Constitutional provisions and laws, internationally recognized treaties and other laws, practical realities and requirements, and historically shaped attitudes. Individuals and groups are either moving between or straddling nations—physically, legally, and socio-culturally. As the people and activities in this zone have a definitive impact on national security as well as on our economy and society, it is important to see this arena as distinct and to manage it according to its requirements.

With this perspective, it becomes easier to examine how counterterrorism measures in this in-between zone are being directed and managed, how governmental and private organizations that operate here do not work well together to provide security, and how new organizational arrangements can be designed to support new terrorist mobility components of the ongoing effort to adapt to new threats and goals. Attention to the direction, management, and organizational structures of a TMS will be fundamental to its success.

A. Obstacles to Effective Management and Organization

Numerous divisions exist today among agencies relevant to acting against terrorists within this border and immigration zone, and some organizations and functions are not adapting as quickly as necessary to the new requirements. To some extent, this is par for the counterterrorism course—the gaps and learning curves that slow progress toward a terrorist mobility strategy are similar to those being confronted in other areas of counterterrorism. At the same time, however, a TMS requires its own specific solutions. The following are some of the most significant management issues that must be addressed at this stage.

- Reflecting the historical gap between the intelligence community and all front-line border services, deficiencies of protections exist in both legal and illegal entry channels. In legal entry channels, all-source scrutiny of travel documents and individuals has not yet been systematically integrated into screening. And for illegal entry channels, the network for information delivery and the relationships between the intelligence (including military) community and border authorities have not been institutionally established. Structural organizational changes are needed that integrate different border zone agencies operationally and managerially, going beyond the typical memoranda of understanding or informal cooperation.
- Reflecting the divide between the crime control authorities and the intelligence community that characterized pre-9/11 information collection and analysis, no formal requirements have been adopted for sharing of information between crime control authorities—the FBI, other law enforcement agencies, and prosecutors—and the terrorist travel intelligence community. Historically, methods of sharing have typically been informal, and these have been demonstrated to be inadequate. There must be formal arrangements, if not specific statutes, to cover the timely sharing of seized travel and supporting and identification documents, the contents of closed case files that have not been made available, and information gleaned in terrorism investigations relevant to mobility tactics. Information-sharing procedures alone are not sufficient; they must be energized by interagency hiring arrangements that go beyond

the traditional exchange of liaison officials. Liaison relationships are too often window dressing that result in less than optimal situations for individuals and agencies and consequently weak support for the underlying missions.

- Reflecting the divide between the FBI and the DHS border and immigration agencies and the parallel divide between the Department of Justice and the Department of Homeland Security, there is no unified program backed up by dedicated, central analytic and policy units to curtail the illicit market in travel and immigration facilitation within the United States, focused on deterring linkages with terrorists. Instead, domestic counterterrorism efforts revolve around the FBI's multiple Joint Terrorism Task Forces and investigations by state and local law enforcement agencies. Absent some fusion and centralization at the policy and operational planning levels, the government cannot effectively attack the mobility dimension of terrorist planning and operations.
- Reflecting the impact of the foreign-domestic divide in intelligence, immigration functions, and law enforcement, a lead department has yet to be designated and staffed to run a high priority interagency program to target terrorist travel facilitators. This contrasts with the evident targeting effort against terrorist financiers, the results of which are regularly visible in news reports. In US embassies abroad, it is not clear whether the United States has more border agency officials focused on human trafficking or on terrorist travel facilitation. There should be a clear prioritization for overseas investigative assignments, taking into account the best available information about the overlap in terrorist and trafficking networks.
- Reflecting the conflation of immigration compliance and enforcement with terrorist mobility investigations, ICE has not yet identified programs specifically dedicated to finding terrorists among visa overstays, student violators, or holders of fraudulent travel and immigration documents. It is insufficient to do plain vanilla immigration enforcement, prioritized by immigration criteria, and wait to stumble into circumstances suggesting terrorism or organized crime. Nor is it adequate to rely on the FBI, since original data, regulatory authority,

expertise, and experience reside in ICE. Highlighting and refining immigration law-based investigations at a level relevant to constraining terrorist mobility, and linking them with a regulatory reform agenda (such as for birth certificates) that responds to the persistent problems identified in compliance and enforcement operations are unique and vital ICE responsibilities.

- Reflecting the dependence on the limited, historical law enforcement tools used against Al Qaeda prior to 9/11, criminal cases against illicit market travel facilitators are generated in field offices; they are not centrally mined for information that may be relevant to understanding trends and patterns, and there is no central analysis to leverage such cross-cutting information to improve enforcement policy and design new regulations. Both the FBI's computer system problems and ICE's lack of focus play a role here. The lack of enforcement and regulatory policy dimensions to the terrorist mobility effort stands in marked contrast to terrorist finance and money laundering, where innovation and high-level attention have distinguished the effort.
- Reflecting further the limited vision of terrorist mobility related crime control programs, anti-corruption efforts in US border services as well as in foreign countries have yet to be elevated to a higher level of policy and operational attention. Corruption, among other crimes, is a more significant vulnerability when contending with terrorism.
- Reflecting the foreign-domestic divide, the historical division between public and private sectors, and conflicts among agencies, foreign airports and other embarkation points are not fully integrated into a screening program focused on individuals or their documents. This is a missing link, especially for screening in countries for which visas are not required, where there are no opportunities for interviews and document scrutiny linked to terrorism intelligence.
- Reflecting the conflation of immigration enforcement policy and terrorist mobility policy, there is a lack of prioritization in several Congressional mandates issued for changes in identification systems.

Driver's license reform, which has been driven by immigration-related concerns, cannot be effective without underlying integrity of US birth certificates, which enable the acquisition of passports and drivers' licenses alike and are therefore a more fundamental concern for counterterrorism.

- Reflecting both historical and potential new management and funding challenges, the respective roles of the military and civilian agencies along US borders (land, sea, and air) between ports of entry are an emerging arena for bureaucratic resource conflict and debate over authorities. Congress has historically funded elements of the Pentagon at much higher levels than it has the immigration, customs, and border patrol services and infrastructure that now play a significant national security role. But the Pentagon is seeking a significant new role at the border through augmented assistance to civilian agencies and establishing new domestic counterterrorism capabilities.⁵¹ Overseas, the military is assisting with border controls through training and other efforts, a change from the 1990s when US Customs inspectors were sent to Bosnia to assist with border-crossing management in lieu of military forces. The appropriate roles and linkages among civilian, military, and intelligence agencies in these venues have yet to be clearly described and debated. For instance, while funding for an effective biometric entry-exit system is slowing, budgets for military-related border functions grow.

This illustrative list of problems is not intended to ignore the efforts being made to address or redress some of these problems in most of these areas. A single highlight of these efforts is Congress's establishment of the Human Smuggling and Trafficking Center to serve as an intelligence fusion center and information clearinghouse for relevant information from all federal government agencies (although not state and local agencies) with respect to the government's efforts to address terrorist mobility, human smuggling, and human trafficking. Although this institution is receiving only partial support, it represents an innovative organizational solution that offers a potentially powerful intelligence and operational platform for a US terrorist mobility strategy, one that can optimize intelligence, law enforcement, diplomatic, and military contributions.

Nevertheless, the list of challenges underscores the reality that discussions about “reorganizing the intelligence community” and “bridging the intelligence-law enforcement divide” and “transforming the military” have generally overlooked the related management and organizational challenges hampering the exploitation of terrorist mobility. Solutions would flow more readily in this arena if terrorist mobility issues found a more prominent and distinct place on the management agenda.

B. The National Security-Immigration Divide

Of all the issues obstructing progress on terrorist mobility, the most fundamental is the historical gap between national security policy and immigration policy. Why a focused approach to terrorist mobility did not develop among intelligence or military professionals some time ago—for instance when the innovation of targeting terrorist funding was adopted—is a question worth examining because it can highlight the attitudes still slowing progress in such an effort. Among the range of possible answers, one clear factor is the cultural divide between the immigration/customs and border control agencies and the civilian and military intelligence communities.

Policymakers and strategists have focused since 9/11 on the “wall” or “seam” between the law enforcement community and the intelligence community, which grew to be an ever more significant obstacle as the government’s ability to “connect the dots” in terrorism analysis became more pressing. For terrorist mobility, the salient divide is between the national security community generally and the immigration and migration policy world. This is causing a drag on a whole range of counter-terrorism measures, especially the ability to intercept terrorists by using the minds, eyes, ears, and technology of border officials.

Prior to 9/11, counterterrorism officials had limited contact with the border agencies. During the first wave of European terrorism in the 1980s, the government compiled information about terrorist travel documents and made it available to domestic border control agencies, airlines, and foreign governments. These resulted in a significant number of successful interceptions at border crossings.

This ancillary initiative was not sustained in its original form or further developed and incorporated into the efforts against Al Qaeda during the 1990s. The intelligence community cooperated only to a limited and sporadic degree with the State Department's computerized terrorist watchlist called Tipoff, the predecessor and core of the post-9/11 terrorist watchlist. When tracking particular terrorists, the intelligence community drew on border agency liaisons and contacts for consular, immigration, and customs information and expertise.

But protocols for building the watchlist were not seen as strategic elements of counterterrorism to be treated as mandatory requirements. Consequently, many names were either not culled from intelligence reports or were not transmitted to the State Department for inclusion in Tipoff. The intelligence community and the FBI engaged with border personnel on espionage or counterespionage cases, with the FBI selectively posting "look-outs" at particular ports-of-entry in intelligence or criminal cases. While criminal cases against terrorists during the 1990s included immigration and travel-related charges, the information underlying these charges about terrorist tactics at border crossings or how they exploited immigration status laws was not compiled and analyzed to be applied in improving regulatory, adjudication, or enforcement policy. Analysis other than to support particular cases was simply not a feature of law enforcement generally.

Before the establishment of the Department of Homeland Security in 2003, few agencies were held in less esteem than those dealing with immigration and border controls, despite solid and respectful working relationships among individuals. Cooperation between the intelligence community and the FBI was obstructed by what came to be known as the "wall," but *both* organizations wished to have as little as possible to do with the legal complexities of the immigration and customs processes and the personnel and operations of the border agencies. These opinions had parallels at the policy level, where there was a sense that immigration and migration policy, and management of the nation's borders, were unimportant as compared with most other policy concerns and missions. Even within the State Department's senior officials, Consular Affairs' visa issuance role was simply not viewed as implicating foreign or security policy.

Beginning immediately after Ahmed Ressam's arrest during the period of the 2000 millennium celebration, counterterrorism specialists made arguments for augmented resources for border agencies and additional focus on immigration investigations of suspected terrorist cell members in the United States. Nevertheless, the interceptions by immigration and customs officials of Ressam in 2000, and that of Mohamed Al Kahtani in summer 2001, which prevented him from participating in the 9/11 attacks, tended to be interpreted as amazingly lucky exceptions. To most policy commentators, the arrests only spotlighted what was assumed to be general incompetence and unreliability, rather than alerting strategists to the emerging centrality of the national security role of the chronically underfunded and politically sensitive border and immigration agencies.

The divide between the national security and immigration and border communities is taking time to dissipate. Border and immigration agencies have been viewed as an unattractive partner by the national security community, which has concerns about infusing classified information into the immigration and border environment or engaging border personnel through substantial training and service in the intelligence community. In a reciprocal way, attitudes within border control agencies have developed contradictory elements of diffidence, resentment, and competitiveness toward the pre-9/11 intelligence community.

Most importantly, although DHS and the Department of State have taken critically important steps to tighten border security, test new immigration law enforcement initiatives, and develop or expand in-house information analysis, terrorist mobility is only beginning to be embraced as a subject for policy attention at senior levels. This has left a troublesome gap. Senior Foreign Service officers still see the consular officers as managing a lesser, service bureau from which they made a timely escape, and they do not associate *policy* with what is regarded as an *administrative* function.⁵³ Consular officers in turn have tended to see security policy as emerging out of an intelligence and law enforcement function that can be differentiated from their specific expertise. In reality, consular officers contribute meaningfully to adjudicative security policy and ought to be recognized as having a critical role here.

DHS is only now establishing a senior level policy office. While it is responsible for some major national issues—immigration and natural disaster response, for example—its counterterrorism mission and supporting organizational structure continue to be defined amidst competing claims by the FBI and military, among other agencies. The intelligence and law enforcement communities (as well as the military) on the other hand do not have the experience in border and immigration control to design terrorist mobility policy on their own.

A fundamental condition for effective policy planning is acknowledging that the largest group of trained government personnel *already in position* and actually available to detect foreign terrorists traveling to and hiding within the United States are not in the CIA, the FBI, or the military. They are in DHS and the Department of State. Indeed, *all* the expert agencies involved with activities that affect US and foreign border zones—DHS’s Customs and Border Protection, ICE, and Citizenship and Immigration Services, among many other offices, State Department’s Consular Affairs, Diplomatic Security, and International Narcotics and Law Enforcement, the Economic Bureau’s anti-corruption officers, International Organizations, regional bureaus, and the interagency Human Smuggling and Trafficking Center, to name only some of them—must be seen as jointly comprising the core of a cohesive cohort against terrorist mobility. Their combined role is *equal in importance* to the FBI, the NCTC, the broader intelligence community’s intelligence efforts, as well as the military’s technical tools in preventing attacks against the United States. If this perspective is not adopted, these agencies’ full capabilities will remain underdeveloped and underexploited, to the detriment of our counterterrorism and homeland security effort.

C. New Arrangements to Attack Terrorist Mobility

New arrangements within government are required to effectively address terrorist mobility. Narrowing the historical foreign-domestic divide in government management, bridging the immigration-intelligence/law enforcement divides, and integrating state and local officials into a broad national effort to develop and apply terrorist mobility information—these major transformations will not be accomplished overnight. Indeed, the challenges are so new that there is not yet an

established expert group of related specialists comparable to thinkers on terrorist finance or nonproliferation specialists that have formed themselves to assist in responding to this problem. How should the government be organized to attack terrorist mobility? There are some building blocks in place and some fundamental questions to be considered.

1. NCTC Strategic Operational Leadership

A basic requirement of a terrorist mobility strategy is that there be someone in charge of its overall design, long-term goals, emphasis at any given time, role in any particular counterterrorism strategic operation, and implementation of planned strategies. The question can be posed in two ways that illustrate the problem. First, the day after the next terrorist attack, who should be held accountable by Congress for the terrorists' ability to travel clandestinely, enter the United States, and gain access to the target? Second, in strategic operational decision making—for instance, an effort to find bin Ladin or to keep Al Qaeda insurgents from entering or exiting Iraq or Europe—who is in charge of defining the terrorist mobility element and ensuring that responsible agencies carry it out?

Congress has already provided at least a preliminary answer to this question. After the president, the individual formally answerable for a terrorist attack on the United States is the chief of the NCTC. Congress has assigned the director of the NCTC a role in counterterrorism somewhat analogous to the chief of staff of the Joint Chiefs of the Armed Forces. The NCTC director is in charge of terrorist-related strategic operational planning. Thus, the NCTC director is the top official reporting to senior political leaders responsible for defending the United States against attacks by terrorists, just as the head of the Joint Chiefs of Staff in the Department of Defense is the senior military official reporting to the political leaders responsible for defending the United States against attack by uniformed military forces. However, the NCTC director reports to the president, not to the head of a cabinet department, on strategic operational matters relating to terrorism and to the director of national intelligence on intelligence matters.

Acknowledging some continuing ambiguities that must be resolved over time, perhaps by more radical change of our cabinet department

structure, for purposes of moving ahead with a terrorist mobility strategy, the outlines and logic of this model is clear enough.⁵⁴ It at least clearly reflects the conclusion that the United States, first, requires a central authority to integrate use of a broad array of counterterrorism measures, many of which are within the authority of civilian agencies, and, second, depends critically for the success of these efforts on intelligence inputs. Thus it makes sense to base the direction and coordinating management of the effort in the first instance in the intelligence community, rather than in the military, law enforcement, border, or diplomatic communities. This does not alter the critical need for participation by each of these in the strategy formulation process and the critical roles each will play in implementing whatever operational strategies are devised.

Consistent with this framework, Congress has assigned the NCTC the job of developing an integrated terrorist mobility strategy. Even the adoption of a broad and systematic approach to reducing all the vulnerabilities in our border and immigration system requires that its elements be prioritized as part of a larger counterterrorism framework, and not principally as an offshoot of immigration policy. Moreover, while advancing an across-the-board homeland security effort to close border and immigration vulnerabilities, a terrorist mobility strategy must be directed as closely as possible against actual threats and the strategic operational priorities of the United States. If the priority is terrorist movement from Europe and Canada to the United States, or into and out of Iraq or Pakistan, then there must be adequate terrorist mobility resources invested in these particular problems. A fence along the US border with Mexico will not provide the solution.

The larger counterterrorism strategy, of which an integrated terrorist mobility strategy is only a part, must be established by the National Security Council. The president, with the NSC and NCTC, decide who poses the greatest threat to Americans—Al Qaeda or successor groups and networks, state-sponsored groups and operations, or groups or individuals within the United States or those located outside the United States—and consequently where US attention and resources must be focused. The border agencies alone cannot assess this threat nor establish the strategic priorities. The weaker the linkage between a

terrorist mobility (or finance or communications) strategy and a broader counterterrorism strategy, the less likely the strategy is to be effective.

For terrorist mobility purposes, the most extensive of NCTC's partner relationships is with DHS. The US border, transportation, and immigration system must be a central focus of national security initiatives aimed at transnational mobile adversaries. Citizens will naturally demand that the screening systems managed by the Department of Homeland Security and Department of State be highly effective in screening out dangerous individuals. After any attack on the United States, the secretary of DHS is nearly as likely as the NCTC director to be held accountable by Congress and the public. Indeed, for the moment the DHS Secretary probably is a more visible official than the NCTC Director and a potential lightning rod for immigration politics and transportation policy debates. Senior officials in the Department of State, FBI, the intelligence community, and Department of Defense also share some accountability for terrorist mobility.

Intense rivalry among all of the involved organizations for control over a TMS would not be surprising, given the substantial authorities of various departments and agencies, particularly DHS and the Department of Defense, the major resources they control, and the fact that problems they deal with have a major impact on terrorist mobility. But close cooperation within the NCTC framework offers the most direct path to optimized defense against and exploitation of terrorist mobility and therefore should remain the undiluted goal. If the NCTC is unable to be successful in effectively directing a TMS, which can be assessed over time, we must look to more radical redesign of government to confront terrorism; otherwise, inevitably, unacceptable weaknesses will be exposed.

2. The Department of Homeland Security's Central Role in Countering Terrorist Mobility

Within this broader NCTC defined framework, DHS has the principal responsibility and major burden for shaping and supporting a terrorist mobility strategy for the US border and immigration system both at the borders and within the United States. Among the key challenges for DHS in this endeavor: defining distinct terrorist mobility related objectives (such as establishing a terrorism-specific, document-scrutiny

capability at border and foreign embarkation points and identifying terrorists among those attempting illegal entries); establishing a much more comprehensive and usable terrorist mobility knowledge framework; bringing about much deeper integration of the border and intelligence communities (including a cross-service for border personnel); continuing to support the development of a linked screening architecture throughout the border and transportation systems, especially the biometric entry-exit system; and taking the lead in policy development concerning the domestic illicit market supporting travel and migration and its links to terrorists.

DHS is still evolving in how it is organized to manage its counterterrorism responsibilities, and there are some key issues to be resolved. Important progress is visible, including in changes proposed in 2005. DHS has the burden of reconciling the resources needed for immigration management and counterterrorism within the border, transportation, and immigration systems. It now has an Office of the Under Secretary for Policy, which can articulate the distinctions and commonalities between terrorism and immigration missions. The role of chief intelligence officer potentially facilitates working with the NCTC to establish requirements for collection and analysis that (1) optimize and further develop the capabilities of different agencies, and (2) ensure full information-sharing concerning terrorist mobility, including entry and access within the United States. But other managerial issues and opportunities remain to be addressed.

DHS is a new organization, and to charge it with undertaking more structural changes is to invite the criticism that ongoing reconfiguring is rearranging the deck chairs and sapping productive energies without concrete benefits. Some patience and long-term views are required. The challenge of reshaping the government to deal with terrorism is a long-term one. But it is better to face important structural problems honestly when we can see them than to ignore them. At present the following problems are visible.

- One managerial issue potentially reducing the ability of DHS to develop a focused terrorist mobility strategy is that, unlike the Department of State, DHS does not have an overall coordinator responsible for counterterrorism. Since Congress formed DHS in

response to the 9/11 attacks with the primary mission of attacking terrorism, it has been assumed, somewhat fuzzily, that DHS as a whole is focused on the counterterrorism mission. The Secretary of State, by comparison, is recognized to have a broad role in pursuing US strategy. And, since 2001, it has become clear that DHS's national security concerns in practice also extend beyond terrorism to other areas equally critical to US well-being—immigration policy, nonterrorist related border security such as readiness to deal with a human pandemic, and natural disaster preparedness and response, to name only those that are currently high on our radar screens. With the DHS secretary necessarily focused on a range of critical issues, absent a designated senior counterterrorism manager, it is unclear who is or should be the key working partner of the director of the NCTC or the Department of State. No one below the secretary has the authority to ensure that DHS operational agencies carry out NCTC priorities for counterterrorism on a day-to-day basis. Without a counterpart, the NCTC (and other departments) must search among dozens of individuals from more than two dozen offices whose senior managers report directly to the secretary of DHS. The lack of a clear partner in senior management makes it hard to appropriately engage DHS in the design of the broader US response to terrorism, including terrorist mobility, where DHS has a leading policy role. Candidates for at least a temporary senior counterterrorism official or pair of such officials to serve as lead partners for the NCTC Director include a senior official reporting to the under secretary for policy—perhaps an assistant secretary for counterterrorism—and the chief intelligence officer. Establishing an under secretary for operations with an assistant secretary for counterterrorism perhaps makes more sense.

- Another new and important role still to be developed is the role of DHS in screening coordination. Screening of individuals occurs throughout the border and immigration systems and at transportation and other access points, but the systems used are not fully compatible. The department's new Office of Screening Coordination and the policy office are positioned to support the interdepartmental process of developing security standards for the issuance of birth certificates (a process the Department of Health and Human Services manages), to implement any federal identification legislation and any system

mandated in the future to enable employers to screen potential employees for immigration and security status. It must also work with the policy office and the science and technology office to develop and/or study additional proposals for further improvements in national identification.

- DHS is well positioned to take the lead in organizing effective terrorist travel document screening and analysis, something that must be done with the intelligence and law enforcement communities. The progress that has been made in organizing a process to optimize the use of watch-listed names—biographic data—to detect dangerous individuals has not been matched by similar progress in using indicators on travel documents and supporting identification documents to detect terrorists who use them and the organizations and individuals supplying these instruments. A new central terrorist travel document screening, analysis, forensics, and information dissemination unit should be established to draw upon and serve border, law enforcement, intelligence, military, and state and local officers. The most suitable host is the DHS Forensic Document Laboratory (FDL), which maintains a definitive global travel and identification document exemplar library and has a history of high technical standards and good working relationships with all relevant agencies, including state and local agencies. FDL has definitive expertise in documents, especially fake documents, and comprehensive knowledge of domestic travel and identification documents and their state and local issuers. Due to reorganization when DHS was established, FDL is currently located within ICE, while the bureau of Customs and Border Protection (CBP) has set up a seemingly redundant Fraudulent Document Analysis unit. Competitive intelligence is useful, but here the material is exceedingly narrow—travel and identification documents. An alternative is to create a single FDL as a companion office to the new Screening Coordination Office. Combining the two functions would unite managers and experts in charge of integrating and designing screening, credentialing, and identification systems, with real-time expertise in the techniques being used to defeat these systems. This should lead to improved screening systems and should bolster efforts to deter and investigate the use of fraudulent documents.

- Adjusting the relationship between the legacy immigration agencies ICE and CBP would be helpful in achieving an integrated approach to terrorist mobility. When the Immigration and Naturalization Service (INS) became part of the new Department of Homeland Security, its civil component was merged with counterpart US Customs Service functions and became the bureau of Customs and Border Protection (CBP); its criminal components were similarly merged within a new bureau of Immigration and Customs Enforcement (ICE). But civil and criminal immigration laws and rules comprise a continuous spectrum of government authority applicable to noncitizens. The more efficient and effective the civil immigration laws and regulatory system are in minimizing illegal entry and residence, the less demand there will be for more severe—and much more costly—criminal enforcement. Therefore, a close and coordinated relationship between the two dimensions of immigration management is critical; criminal trends can help rule-makers decide what new actions to take, and adjudicators and regulators can point out where more criminal enforcement is needed. Even if ICE takes on broader enforcement roles within the Department of Homeland Security, it makes sense for the two bureaus to be merged.

- A structure that requires twenty-six entities to report directly to the Secretary seems unsustainable and potentially undermines central direction of policy.

3. The Department of State's Leading Role in Shaping an International Terrorist Mobility Strategy Within the NCTC Counterterrorism and Terrorist Mobility Framework

This report has omitted the full discussion required of the bilateral, regional, and international dimensions of a terrorist mobility strategy. The State Department is already contributing substantial components of such a strategy itself, including such sensitive innovations as denying visas to corrupt border officials. Clearly, the State Department has the leading role in shaping an international terrorist mobility strategy within the framework set by the NCTC and NSC. Intelligence community components, DHS and its operational bureaus, the Department of Justice, and the FBI necessarily will play a large role.

In addition to the ongoing strengthening of counterterrorism measures in the visa issuance process, areas for action include: providing border-related foreign assistance; developing terrorist mobility related agendas for the G-8 and other regional organizations; designing bilateral, regional, and multilateral treaties related to terrorist mobility (as well as exploring new or revised United Nations instruments and programs); coordinating concerted diplomatic efforts focused on access to terrorist watchlists; placing US enforcement officials to support a strategy to shrink the illicit travel market; establishing terrorist mobility related anticorruption initiatives; and contributing to information development concerning terrorist and criminal mobility and broader travel fraud trends to which they may be related.

As the Department of State pursues global counterterrorism diplomacy, it must be organized to build a mobility element into *each* of its key counterterrorism strategic dimensions: safe havens, terrorist organization travel facilitators, and underlying conditions terrorist organizations may exploit, like widespread corruption, as well as measures to prevent access to the United States.

4. The Human Smuggling and Trafficking Center (HSTC)

The HSTC is an entity well situated to become the permanent host for an interagency effort to target terrorist travel facilitators, and it should be re-named to reflect its terrorist mobility mission as the Terrorist Travel, Human Smuggling and Trafficking Center. At present it remains an experiment in government organization. Chartered to develop information about human smuggling and trafficking, and now terrorist travel information and intelligence as well, it is governed by a board from three cabinet departments and must report to the NCTC on terrorist travel matters. The 2004 intelligence reform legislation requires the HSTC to serve as an intelligence fusion center and information clearinghouse for relevant information from all federal government agencies with respect to the government's efforts to address terrorist mobility, human smuggling, and trafficking. The federal government has yet to take full advantage of this institution. The opportunities offered by fusion and functional clarity will be undermined if the HSTC is denied an effective leader by senior officials, or becomes a budget orphan, with departments inclined to let the others pay and a lack of consistent supervision and congressional focus.

To have a chance at success, a senior seasoned leader is required, and supervisory authorities—NCTC, the director of national intelligence, and the Office of Management and Budget, as well as the trio of cabinet departments—must help with the budget and ensure contributions from other entities. As an intelligence fusion unit, the HSTC has no agents to pursue cases. This would be less of a problem if there were investigative and policy organizations elsewhere whose missions included systematically following up on the intelligence developed by the HSTC, but no such follow-up is ensured because there is no designated operational unit.

5. Investigative Resources to Pursue Terrorist Mobility Related Transnational Cases

The lack of a designated terrorist travel *investigative* organization can be traced back to the inherent ambiguities in DHS and FBI authority over terrorist mobility related operations. To pursue terrorist mobility related cases based on information developed by the HSTC—or by any other entity—the FBI, ICE, and the State Department’s Diplomatic Security arm could establish a joint Terrorist Mobility Operations Unit with agents available to assist major overseas investigations relating to terrorist travel. Such investigations may not *necessarily* involve travel aiming directly at the United States but would be conducted jointly with allies. These agents should not be tied to local US Joint Terrorism Task Forces (JTTFs) or domestic FBI offices. Instead they should be free to travel anywhere in the world to support investigations.

Several agencies have expertise that should be combined. The FBI has the primary counterterrorism investigative authority, but ICE (and CBP) personnel have much deeper and broader ongoing exposure to, and expertise in, immigration and migration practices and in the use of civil regulatory and enforcement tools. Agents in the diplomatic security bureau of the State Department have expertise in passport and visa fraud aimed at the United States. A more coherent framework for international terrorist mobility operations, based on threat assessments and targeting from the HSTC, would optimize these agencies’ existing resources. The energy-sapping acrimony that has surrounded the staffing of terrorist finance investigations should be avoided.

6. Investigative Agencies and Terrorist Mobility Information

An urgent challenge of the FBI and other law enforcement investigative agencies is to provide access to terrorist mobility information in investigative files to analytic units that are focused on developing information about practices and trends. This must include both the sharing of seized travel and identification documents or their images, and the fruits of interviews and seizures. Agencies developing analysis of and expertise in immigration and terrorist travel can then provide finished products to FBI and other investigative units—the JTTFs and headquarters units, the Drug Enforcement Administration (DEA), the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and others—which conduct investigations in the United States and in foreign countries. Absent a computerized file system, information sharing should be performed manually. Since just this kind of gap was a factor in the 9/11 attacks, any continuing absence of travel-related investigative information merits intervention by the director of national intelligence as an exercise of his authority over “information architecture.”

7. State and Local Agencies

Development of a terrorist mobility focus by the federal government should be matched by the inclusion of a terrorist mobility dimension into existing planning for state and local fusion centers, including for training and operational linkages.⁵⁵ State and local agencies may be highly informed about travel, transportation, and immigration-related frauds that relate directly to terrorism. For instance, local police are likely to be exposed to the types of visas used by residents who are suspects in terrorism investigations; they do not, however, have the legal authority or policy leadership to take action.

The fact that terrorist mobility is a new field places a major burden on top-level strategy and policy planning units, which in turn have to reach out to a variety of experts to help design new business processes that move beyond the historical divisions among intelligence, law enforcement, and immigration adjudications, and foreign and domestic law enforcement relating to immigration. These experts are not, for the most part, outside the agencies themselves; they are government officials already on the front lines who encounter terrorists and travel and immigration fraud in the course of their daily intelligence, border, and investigative duties.

Only a system that provides strategic direction and drives implementation in that context, combined with ongoing input from those knowledgeable about the opportunities and frustrations of actual operational activities, will be successful.

V. NATIONAL STRATEGIC AND STATUTORY FRAMEWORK

A terrorist mobility strategy, like a terrorist finance strategy, is primarily operational in nature. It provides a conceptual framework for developing and harnessing an array of tools relating to travel, transportation, and immigration that are not altogether new but that are newly significant against adversaries that present themselves as “microtargets.”⁵⁶ These tools compose a critical functional component of counterterrorism.

A TMS is significant because it provides critical support to each element of an existing counterterrorism strategy. For example, a TMS is a supporting element of a counterterrorism strategy that posits simultaneous attack on violent ideology, on underlying political and social conditions, and on operational elements. Beyond that, a TMS can be used systematically to support specific strategic priorities—on the Afghan-Pakistani border, the Iraqi border, or in homeland security. In security policy generally, whether the focus is terrorist leadership, safe havens within sovereign states, travel by recruits and operatives, transnational criminals feeding off global markets, or virus-carrying travelers, the techniques of a terrorist mobility strategy—precise knowledge, attack on travel facilitation nodes, transparency in legal channels, reduction of terrorists’ access to illegal channels, and so forth—are applicable.

Like terrorist finance or other elements of operational counterterrorism, a TMS has implications for higher levels of US strategy, for “grand” or “macro” strategy. Prior to 9/11, antimoney-laundering and terrorist finance techniques attracted opposition from national economic

policymakers because these methods implied enhanced regulation of access to US financial institutions and therefore were perceived as potentially reducing financial flows to United States and chilling the global financial market. Even today, criticism of the costs of a terrorist finance strategy periodically emerge from the business community.⁵⁷

Similarly, a terrorist mobility strategy may be designed to be consistent to a greater or lesser degree with a spectrum of approaches to our role in the world. Strong preference for unregulated markets and for a strict separation between the free market and government security responsibilities will tend to diminish support for public and private investment in screening in legal border and transportation channels. These attitudes may be reflected in an ongoing hesitation to invest in technology and infrastructure at US consular posts and ports of entry as an essential national security requirement, comparably important to the next generation of military hardware. Strong belief in the exercise of US sovereign power, instead of in the United States becoming a leader in the formation of coalitions, will tend to deemphasize systematic efforts to develop new legal frameworks for cooperative counterterrorism defenses in international travel channels in favor of unilateral actions and policies. Greater emphasis on nativism or American exceptionalism, rather than vindicating human rights embodied in treaties, is more consistent with an emphasis on reducing or blocking immigration across the board rather than on heightening effectiveness against entry of dangerous individuals.

But these types of arguments at a high and general level of US strategy—toward more or less unilateralism, more or less regulation of markets, and more or less concern for national cohesion and adherence to internationally recognized formulations of human rights—while an important dimension of political dialogue and strategy development, are not substitutes for the hard, detailed work of figuring out step-by-step how to use terrorists' and criminals' need to travel against them. Arguments about the appropriate degree of US receptivity to immigration cannot substitute for effective counterterrorism. While to some extent the macrostrategy can guide a terrorist mobility strategy, to a very real degree what *works* against terrorists and international criminals at the individual level must also be recognized to be a crucial driver of the

larger strategy. What works to constrain terrorist mobility can be discovered by building in systems that routinely provide answers to such questions as, “How many correctly targeted terrorist suspects were identified this year, and by what means and where?”

Terrorist mobility has a place in the major discussions of strategy that articulate visions and plans for the United States, and set forth counterterrorism and homeland security strategy.⁵⁸ It is therefore worth looking at what these important statements do say that relate to the subject.

The *National Security Strategy of the United States of America* (2002) is the most fundamental strategic document issued since 9/11, and is controversial in its announcement of a new doctrine of preemption. It commits the United States to strengthening alliances to defeat global terrorism and to working to prevent attacks against us and our friends by various methods. Declaring that in a globalized world our society must be open to people, ideas, and goods from across the globe, it states that “our systems of movement” is among the characteristics of our society we most cherish and that we must protect.⁵⁹ It is unclear from this brief exposition whether this strategy envisions the United States assisting in securing global travel channels, but it is consistent with containing terrorist mobility while generally protecting freedom of movement.

The *National Strategy for Homeland Security* requires updating but is still a useful and influential document that provides the most thorough examination of homeland security and domestic counterterrorism available to the public.⁶⁰ It establishes border and transportation security as one of three critical defensive mission areas, and its concept of this mission has definitively shaped policy. It fully captures the multiplicity of security challenges that border and critical infrastructure access points must address, provides a compelling long-term vision, and alludes to many policy directions that remain important and undeveloped, including a number mentioned in this report.

At the same time, that vision does not distinguish adequately between specific requirements that have emerged for counterterrorism and other homeland security requirements. It does not recognize terrorist mobility as a functional component of counterterrorism, analogous to terrorist

finance, nor does it draw out the operational level generally as integrated planning distinct from both tactical and long-term strategic considerations. Consequently, it underestimates the essential role in counterterrorism that border, transportation, and immigration authorities must exercise—in our legal and territorial border zone, in foreign countries, and in the United States. Rather than presenting a view of counterterrorism that integrates a number of authorities—an essential requirement—the strategy perpetuates the view that the intelligence informing our efforts to secure travel, entry, and residence channels will be conducted within the traditional intelligence community, with an enlarged, domestic intelligence role for the FBI. A successor version of the strategy should identify terrorist mobility as a vulnerability to be exploited, focus on what homeland authorities must do to defend against and exploit terrorist operational approaches generally, and replace a traditional view of intelligence with an expansive view of new knowledge development methods.

The *National Strategy for Combating Terrorism* (2003) affirms the goal of accommodating an enhanced flow of people and goods while identifying the few dangerous, criminal, or otherwise unqualified travelers through screening measures at border and critical infrastructure points. Preventing unimpeded transit of terrorists is identified as an important aspect of denying terrorists sponsorship, support, and sanctuary, and taking steps to do so is noted as a needed “international standard of accountability,” without indication of the process by which these standards should be promulgated.

Although the strategy alludes to terrorist movements several times, overall it seriously underestimates the vulnerability and opportunities associated with terrorists’ need to be mobile. Members of Al Qaeda are mistakenly described as traveling “with the ease of a vacationer or business traveler.” In fact, Al Qaeda, in the period up to 9/11, dedicated significant, specialized resources and in-depth attention to the travel problem. In the case of the 9/11 plot, Al Qaeda leadership prepared elaborately for entry into the United States and was unable to move into the country all of the operatives selected for the attacks. Terrorist networks generally work hard to execute travel without running into problems.

Since the vulnerability exposed by the need to travel is not recognized, it is not surprising that, although it commits to eliminating specific capabilities as a means of “destroying terrorists and their organizations,” the ability to move people is not enumerated as a capability to be attacked. Similarly, the importance of breaking the nexus between drugs and terror is cited—but the nexus between human smuggling, trafficking, and terrorist mobility is not discussed.⁶¹

The *Strategy for Homeland Defense and Civil Support* (2005) commits the Department of Defense to an active layered defense in the geographic approaches to US territory, and within the United States, including by detecting, identifying, and tracking emerging threats in all operational domains.⁶² The strategy’s terms are ambiguous, and the strategy itself does not mention using terrorists’ need to be mobile against them.

Although it is not clear whether the role it envisions is limited by being tied to the goal of protecting military forces, the Department of Defense acknowledges that it is not responsible for stopping terrorists from coming across our borders or through our ports or from hijacking aircraft, or arresting terrorists in the United States. A suggestion that the military should operate a border control system parallel or superimposed on the civilian border control system would be alarming from a resource and legal authority perspective. The United States needs an all-in-one border system that moves traffic through and screens effectively; its counterterrorism components require strategic operational supervision by the National Counterterrorism Center.

The most recent Department of Defense strategy, the *National Military Strategic Plan for the War on Terrorism (NMSP-WOT)*, injects both clarity and confusion into the mobility-related counterterrorism strategy.⁶³

It makes progress in that it clearly identifies “movement” as one of nine terrorist operational elements that require further detailed study—mapping, identifying specific networks, developing action plans, designing metrics, and tracking progress; calls for movement to be addressed at the operational and tactical levels; emphasizes that the networked nature of terrorist organizations means actions at the regional level can be significant; and in numerous ways emphasizes the role of working with other countries. These are among the elements of the *NMSP-WOT* that advance national strategy relating to terrorist movement.

Where the strategy sows confusion is in its articulation of what actions are required to address terrorist movement and the respective roles of various government arms in leading, designing, and carrying out these activities. The *NMSP-WOT* characterizes movement as including “couriers, movement corridors/transit points; relative anonymity; organic and commercial transportation; popular support; and illicit/criminal trade mechanisms.” To take action against these functional elements, the military assigns itself the broad role of “detering, detecting, and interdicting terrorists before they can reach the United States and protecting potential military targets in the homeland,” while “[l]aw enforcement and diplomatic instruments lead the effort to deny enemy transit across borders and to protect likely targets in the United States.”

But it is left unexplained how these particular problems of mobility—terrorists’ use of couriers and exploitation of transit points, for example—relate to the military’s actual capabilities and authorities, fighting wars or otherwise. The military has a key role in interdiction of terrorists seeking to enter combat zones, such as in Iraq; in detecting terrorists in the Afghanistan-Pakistan border area; and in training of foreign military border protection forces; among other important functions relating to terrorist mobility. But terrorists aiming at the United States travel mostly in channels under civilian authority, potentially using commercial, migrant, or criminal pathways. The *NMSP-WOT*’s explanation of the organization of forces to deal with terrorist movement leaves ambiguous the military’s operational relationships with the National Counterterrorism Center, which provides strategic operational planning, prepares terrorism analysis, and supplies the terrorist watchlist, among other core functions relating to terrorist mobility; with the customs, immigration, and transportation officials, who are not members of law enforcement but who design the systems, conduct the screening, and perform analysis centrally and in consulates, ports of entry, and within the United States; and with the range of law enforcement and immigration and customs officers at US borders and overseas who patrol the border and attack the illicit market in travel services using a range of methods, including traditional crime control and intelligence. This disjuncture is also present at the strategic level—the *NMSP-WOT* omits from its flowchart depicting the national strategic framework a line to the *National Strategy for Homeland Security* or to the role of the National Counterterrorism Center as the

strategic operational center for US counterterrorism. Perhaps sewing all these seams is too much to ask from a strategy intended to focus solely on military operations. Nevertheless, these questions must be addressed if the abstractions of the *NMSP-WOT* are to be given life on the ground.

A growing focus on a cohesive, government-wide approach to terrorist mobility in strategic circles is inevitable. The main impetus is Congress's mandate in the *Intelligence Reform and Terrorism Prevention Act (IRTPA)* that the National Center for Counterterrorism (NCTC) produce a classified and unclassified terrorist travel strategy and take action in a number of areas to support such a strategy. Congress's directions in IRTPA are summarized below.

Terrorist Mobility Strategy and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)

Section numbers refer to IRTPA.

Findings. International travel is dangerous for terrorists because they must surface to pass through regulated channels, present themselves to border security officials, or attempt to circumvent inspection points. Terrorists use evasive but detectable methods to travel, such as altered or counterfeit passports and visas, specific travel methods and routes, liaisons with corrupt government officials, human smuggling networks, supportive travel agencies, and immigration and identity fraud. Routine operations of the immigration system, investigative insights gained since 9/11, and classified intelligence collection and analysis are all relevant to border security (Sec. 7201(a)).

Strategy. The director of the National Counterterrorism Center shall submit to Congress unclassified and classified versions of a strategy for combining terrorist travel intelligence, operations, and law enforcement into a coherent effort to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility domestically and internationally. The strategy shall be developed in coordination with all relevant federal agencies (Sec. 7201(b)).

Assessments. The director of the National Counterterrorism Center should include in his report to Congress an assessment regarding the

vulnerabilities within the United States and foreign travel systems that may be exploited by international terrorists, human smugglers and traffickers, and their facilitators. The Human Smuggling and Trafficking Center shall submit to Congress on an annual basis a strategic assessment regarding the same vulnerabilities (Sec. 7201(b)(1); 7202(c)(4)).

Elements of the strategy. Elements that may be part of the terrorist travel strategy, along with any related mandated steps, include:

- **Development of terrorist travel knowledge**—the intelligence and law enforcement collection, analysis, operations, and reporting required to identify and disrupt terrorist travel tactics; a program for collecting, analyzing, disseminating, and utilizing information and intelligence regarding terrorist travel tactics; identifying which federal intelligence, diplomatic, and law enforcement agencies will implement each element; information-sharing actions among DHS and state border agencies and other classified and unclassified sources of terrorist travel intelligence, including procedures to ensure that NCTC receives timely terrorist travel intelligence from border authorities, law enforcement officers, and military personnel; and dissemination of intelligence and operational information among DHS, the State Department, NCTC, HSTC, and other appropriate agencies (Sec. 7201(b)(3)(A), (B), (G), (H)).
 - A significant increase in funding allocations by the director of national intelligence for terrorist travel related collection and analysis (Sec. 7201(e)); and
 - A DHS program to oversee implementation of DHS’s terrorist travel intelligence-related responsibilities within the department and between DHS and other appropriate federal agencies, developed in consultation with the director of the National Counterterrorism Center (Sec. 7215).
- **Establishment of a terrorist travel document program**—development of a robust travel document screening process to intercept terrorists, specifying the technology and procedures required to integrate travel document and other terrorist mobility intelligence into front-line border operations, law enforcement operations, and military force protection, including provisions to digitally transmit suspect travel documents from border and immigration access points to a document screening center with terrorist travel expertise (Sec. 7201(b)(3)(D), (K), (N)).

- A technology plan to support travel document authentication (Sec. 7201(c));
- The establishment of at least twenty-five preinspection stations at foreign airports by June 2006 (Sec. 7210 (d)); and
- A study of the role of passports reported lost or stolen in terrorist travel, and of the feasibility of establishing a real-time international information system identifying persons to whom passports are reissued (Sec. 7217).
- **Deployment of terrorist travel experts**—a program to provide each consular post, port of entry, and immigration benefits office with a counterterrorist travel expert trained and authorized to use the relevant authentication technologies and cleared to access all appropriate immigration, law enforcement and intelligence databases; and to ensure related appropriate consular officer access to intelligence and law enforcement information (Sec. 7201(b)(3)(J), (M)).
- **Training**—the training and materials required by border officials to detect and disrupt terrorist travel (Sec. 7201(b)(3)(C)).
 - A comprehensive terrorist travel training program review, update, and implementation to be undertaken by the secretaries of DHS and Department of State, including provision of assistance to state, local, and tribal authorities and the private sector (Sec. 7201(d)).
- **Dedicated resources for operations against terrorist travel facilitators**—the addition of operational capabilities to the Human Smuggling and Trafficking Center to combat terrorist travel and measures to ensure sharing of operational information among DHS, the Department of State, NCTC, and other appropriate agencies (Sec. 7201(b)(3)(F),(L)).
 - **The Human Smuggling and Trafficking Center.** Under the authority of the secretary of state, the secretary of homeland security, and the attorney general, HSTC is to serve as the focal point for interagency efforts to address terrorist travel; function as a clearinghouse with respect to all relevant information from all federal government agencies in support of US efforts against terrorist travel, and human smuggling and trafficking; convert information into tactical, operational, and strategic intelligence; ensure cooperation among all relevant agencies; support the National Counterterrorism Center, as well as prepare the annual assessment (Sec. 7202).

- **The Visa and Passport Security Program.** The Bureau of Diplomatic Security at the Department of State is to establish a strategic plan to target and disrupt individuals and organizations within the United States and in foreign countries involved in the fraudulent production, distribution, and use of passports and visas, with an emphasis on terrorist linkages (Sec. 7218).
- **Foreign assistance**—the use of foreign technical assistance to advance border security measures and law enforcement operations against terrorist travel facilitators (Sec. 7201(b)(3)(I)).

Other required actions:

- A report on strategies for increasing collaboration with allies in the exchange of terrorist information (Sec. 7210 (c));
- Pursuit by the president of an international agreement to track and curtail terrorist travel, focused on lost, stolen, or falsified documents; related standard-setting by the International Civil Aviation Organization; and other United Nations Security Council resolutions relating to terrorist travel that would augment UN antiterrorism efforts (Sec. 7204);
- A plan to require US citizens and citizens of all other nations by January 2008 to present passports or other documents upon entry into the United States, including special provisions for border communities and registered traveler programs to expedite border crossing for frequent travelers; (Sec. 7209)
- Extensive, detailed planning for acceleration of the biometric entry-and-exit data system (Sec 7208); and
- The establishment of federal minimum standards for birth certificates by the secretary of health and human services (Sec. 721 I).

These provisions do not exhaust the post-9/11 provisions relevant to constraining terrorist mobility in the IRTPA, the USA PATRIOT Act, various authorization and appropriations laws, and immigration legislation. They do, however, provide a sense of Congress's interest in a terrorist mobility strategy.

Congress's mandate and the internal process generated by it suggest that there is reason to believe that when the next government-wide counterterrorism strategy is written, it will include a terrorist mobility strategy as one of its key operational levers. But the contents of the Department of Defense's *NMSP-WOT* suggest that the major challenges for this strategy will be to bridge what appears to be a growing gap between the military's view of its role in counterterrorism and the leadership roles assigned by Congress to the National Counterterrorism Center and the Department of Homeland Security. A secondary but important challenge is to integrate the FBI's counterterrorism responsibilities with DHS's border and immigration capabilities to create an effective counterterrorism force in the border, immigration, and transportation zone.

The lack of a role for mobility in a broad counterterrorism strategy does not mean that various agencies are not already taking significant actions that would support such a strategy. Indeed, it seems fair to assume that significantly improved security in our legal entry channels and greater focus on blocking illegal channels already must have forced changes in terrorists' operational thinking during the four years since the 9/11 attacks. The challenge now is to integrate the diverse elements already being pursued, assign them higher priority, advance them through coordinating management, and support them with more resources.

CONCLUSION

Exploiting terrorists' need for mobility and developing an integrated terrorist mobility strategy comparable to a terrorist finance strategy are fundamentally simple ideas, and so obvious that one may quickly choose to dismiss them. Many in government agencies would insist they are already doing all that can be done anyway. The policy community might well suggest that current approaches to immigration policy, national security, and homeland security already effectively provide countermeasures to terrorist mobility. There is, they may say, nothing new here.

And indeed, perhaps far more terrorists are caught due to vulnerabilities exposed by their movements than by their financial arrangements, although how methods of detection stack up does not appear to be a subject of monitoring and assessment in our larger counterterrorism effort. But surely the success we have had so far should encourage us to take a closer look at—and maximize—the opportunities. A strategy that takes a distinct and systematic approach to exploiting the potential vulnerabilities of the terrorist mobility requirement would enable efforts that are relatively small-scale and disparate to become a powerful component of global counterterrorism.

To be effective, that strategy must distinguish counterterrorism from immigration policy. Our current immigration crisis is largely rooted in an ongoing large-scale influx of low-wage workers from and through Mexico and Central America. By contrast, the terrorist threat to the homeland (as well as to our citizens and interests abroad), is characterized by small cells that come from around the globe—not just from the Middle East but from or through Canada, where the government has identified numerous Islamist militant groups; from Europe with its alienated Muslim population groups; from southern cone transit points—Caribbean, Mexican, Central American, and Latin American—and from many other areas of the world. Moreover, an ample supply of homegrown violent individuals exposed to the violence-colored rhetoric of extremism in US prisons and in mosques provides a resource pool for these cells. Regardless of what we achieve in stabilizing the level and orderliness of immigration—and we will not achieve a perfect equilibrium—there will continue to be a vital requirement for focused counterterrorism efforts throughout the border, immigration, and transportation systems.

At the policy and program levels, the new significance of border and other screening points for preemptive operations is gradually being absorbed by the national security community. Border and transportation controls are recognized as crucial in protecting the population from a range of security problems—the smuggling of weapons of mass destruction, illegal financial and product flows, and epidemics. But borders, border personnel, and the movement of people are still overwhelmingly treated as the purview of the immigration debate and its current crisis. Although

the immigration environment is a distinct sphere for counterterrorism, a fact recognized in practical terms by the establishment of DHS, it is still not fully integrated at the policy and strategic levels. There also remains an unfortunate tendency to deprecate border personnel, lingering from a period in which immigration and migration policy were not widely seen as top-tier policy subjects or relevant to national security. A respect for the expertise and significant role of border and immigration personnel should be promoted and supported within an integrated counterterrorism strategy.

Also slowing a terrorist mobility strategy is a tendency to see intelligence and immigration policy as an oppositional pair operating in separate realms. Terrorist mobility, however, cannot be dealt with principally through cold war intelligence collection methods, although many of the classic practices are necessary ingredients. Nor can it be dealt with by adjusting immigration laws and practices to admit or exclude more workers, visitors, refugees, or asylees, although how we control our borders and shape our society, and where we stand on global migration issues, are highly relevant. Neither intelligence nor immigration policy alone or immigration policy simply given more intelligence, will be adequate as a defense against asymmetric warfare and supercriminals. What is needed are countermeasures embracing integrated tools, specifically designed to exploit the ability of terrorists and criminals to move at will. These integrated tools can draw on many existing capacities, including both intelligence and immigration systems.

There is a deepening tactical and policy consensus on the need for security protections methodically layered into the different aspects of our border system. But concerns about privacy, immigration enforcement policy, and trade policy combine to impede an objective look at counterterrorism imperatives. A biometric-based entry-exit system that covers *all* US border crossings, for example, evokes skepticism instead of being taken as a compelling national security challenge. A program to place an *immigration* screening obligation on state motor vehicle departments needs to consider which *counterterrorism* measures should exist in the driver's license issuance and enforcement system—and whether, as a practical matter, birth certificate security is a prior requirement more directly relevant to constraining terrorist mobility.

The questions to be asked clearly are, What does each layer contribute to countering terrorist mobility, and how does this mechanism relate to other important goals? Immigration control mechanisms are almost treated as substitutes for counterterrorism, which they are not. The government offices that might begin to tackle these planning and strategic problems—like the DHS Screening Coordination Office, the DHS Office of the Under Secretary for Policy—are just now being designed into being.

The need for a crime control program aimed at denying terrorist access to the illicit infrastructure is being lost while the debate continues about the right level of immigration and how to enforce it. This contrasts with the priority given to a multifaceted approach to banking integrity, money laundering, and terrorist finance. Entry and enforcement policies lack a well-developed terrorist-specific dimension distinct from but resting on sound screening and investigative practices to find nonterrorist related immigration violations.

Notwithstanding the fog that the immigration crisis imposes on terrorist mobility policy, there is an emerging, coherent set of countermeasures that respond to a type of enemy that moves individually or in small groups. Designing a cohesive, comprehensive approach to constraining terrorist mobility means shaping the evolution of current practices and programs toward:

- Knowing more about terrorist mobility and residence tactics;
- Deploying more resources historically associated only with the intelligence community to track and disrupt terrorist mobility, while simultaneously increasing efforts to establish lawful, common mobility-related counterterrorism practices with and among allies;
- Treating the borders of the United States and those of other states as critical, powerful, and severely underused counterterrorism resources, not merely as lines drawn against illegal immigration (or military invasion);
- Prioritizing the illicit market in travel, transportation, and immigration-related services as an arena for deterrence, enforcement, and domestic and international lawmaking;
- Confronting the need to improve our ability to know who is in the United States; and

- Highlighting the border and immigration system as a priority for planned postattack review.

As with terrorist finance and the field of nonproliferation, terrorist mobility requires the use of specialists from the full range of government departments—intelligence, civil immigration and border authorities, law enforcement, and the military—and from across the private sector to contribute to an arsenal of new countermeasures. The organizations on which we are relying for intelligence, crime control, and immigration management unquestionably have the capacity to develop into an integrated force targeted on terrorist mobility. The National Counterterrorism Center and the director of national intelligence, the Department of Homeland Security, and the Department of State are the agencies that must take the lead, with full engagement across the intelligence community, the FBI and Justice Department, and a range of other departments and agencies. For the time being they have sufficient authority to make significant progress. In the future, the need for much more substantial change may become evident.

Military science has long dedicated major resources to develop detailed, comprehensive knowledge of enemy movements. In this tradition, the cycle of terrorist mobility intelligence—learning about the enemy’s movements, acting defensively and offensively, assessing and revising operations—would seem to be an obvious prescription. It nevertheless presents a considerable challenge for government today, because we are not yet organized to produce the collection, analysis, reporting, and operational planning about terrorist mobility. Building new programs requires establishing new organizations that fuse the capacities of historically autonomous agencies carrying out counterterrorism, crime control, immigration regulation, and regulation of the transportation industry. A terrorist travel document center in DHS (backed up by a counterpart intelligence community entity), the new DHS Screening Coordination Office, the promising Human Smuggling and Trafficking Center—these can be 21st century-style information hubs that oversee or supply the management and coordination of information standards and strategic and tactical intelligence to “connect the dots” and allocate resources optimally among all relevant organizations.

There has been extensive commentary since 9/11 on the need to redesign relationships among intelligence and law enforcement authorities. For the new centers and larger departments to be effective, however, comparable attention must be paid to strengthening relationships among existing intelligence and immigration and border control authorities and law enforcement agencies in the terrorist mobility field. We must ask hard questions about the role of the military with respect to border and immigration security. A priority is for the FBI to match its powerful investigative capabilities with equally vital contributions to the terrorist mobility intelligence cycle. They can do this by developing a system to provide relevant information in its investigative files to tactical and operational analytic units focused on terrorist mobility.

A terrorist mobility strategy has to be dynamic in a practical way. In the current environment, there are too many new requirements and initiatives piled on top of one another that lack adequate and commensurate resources. Good ideas are not lacking in Washington, and the project of remaking national security to deal with terrorism has brought about an outpouring of contributions and initiatives. But even good ideas are badly timed if they do not allow earlier initiatives a chance to develop in stages—to mature, falter, recover, and make good on their promise. Massive new programs are being developed. Congress has mandated a classified and unclassified terrorist travel strategy. The directions suggested in this report are not intended to ignore or preempt current efforts not mentioned here. The objective is to provide a stronger, more effective counterterrorism framework that can be debated and further developed.

ENDNOTES

1 The 9/11 Commission recommended that terrorist travel become a strategic focus for counterterrorism, stating that targeting terrorist travel is at least as powerful a weapon against terrorists as targeting their money. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton and Company, June 2004), 385. Terrorist travel and residence tactics are described throughout the *Report*, and are elaborated in a staff report, National Commission on Terrorist Attacks Upon the United States, *9/11 and Terrorist Travel* (Franklin, TN: Hillsboro Press, June 2004), and referred to in Steven Sasser, ed., *The 9/11 Investigations*. “Staff Statement No.1: Entry of the Hijackers into the United States,” Public Affairs (2004). This paper further develops this concept. As such, it builds on the work of the 9/11 Commission, including work by Thomas R. Eldridge, Janice L. Kephart, Walter T. Hemphill II, Kelly Moore, and Joanne Accolla. The Commissioners, Philip Zelikow, Chris Kojm, Dan Marcus, and Steven M. Dunne, guided this work, and they and numerous other members of the staff contributed significantly to the commission writings relating to the movements of the 9/11 conspirators. Apart from the 9/11 Commission publications, terrorist travel or terrorist mobility, the broader term adopted here, is not addressed as such in terrorism literature. For example, exploiting terrorist mobility is not among the enumerated counterterrorist instruments presented in Paul R. Pillar, *Terrorism and U.S. Foreign Policy* (Washington, DC: Brookings Institution, 2001). Philip B. Heymann, *Terrorism Freedom and Security* (Cambridge, MA: MIT Press, 2003), 49-58, sets forth a schema for denying terrorists access to targets as a means of threat reduction and protection from unidentified terrorists. Stephen Flynn, *America the Vulnerable* (New York: Harper Collins and Washington, DC: Council on Foreign Relations, 2004) further develops previous work outlining a layered homeland security system that integrates border and transportation systems. The broader terrorist mobility strategy described here would continue to strengthen these defensive approaches but as part of an integrated offensive, defensive and deterrent operational strategy aimed at constraining mobility.

2 The impact of 20th century achievements on 21st century strategy and law are examined in depth in Philip Bobbitt, *The Shield of Achilles, War Peace and the Course of History* (New York: Knopf, 2002).

3 James D. Wolfensohn, “A New Global Balance: The Challenge of Leadership” (Address to the Board of Governors of the World Bank Group, Joint Annual Discussion, Dubai, United Arab Emirates, 2004).

4 Department of Defense, *Strategy for Homeland Defense and Civil Support*, June 2005.

5 Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, Subtitle B, Sec. 1021 (F)(f); Sec. 7201; Sec. 7202-7220.

6 For analysis and proposals on guidelines to protect security and liberty in some of the arenas touched on in this paper, see Philip B. Heymann and Juliette Kayem, *Protecting Liberty in an Age of Terror* (Cambridge, MA: MIT Press, 2005); David Martin, Testimony before the 9/11 Commission, Dec. 6, 2003; Khaled Abou El Fadel, Testimony before the 9/11 Commission, December 6, 2003.

7 How a few of the 9/11 conspirators were blocked from entry to the United States during the process of applying for visas and/or at a port of entry is described in the *The 9/11 Commission Report* (see n. 1) and in the supplemental report, *9/11 and Terrorist Travel* (see n. 1).

8 Luis Redueles and Manuel Mariasca, “Los jefes Al Qaeda usan pasaportes españoles.”

9 For some discussions relevant to this topic, see Hillel Fradkin, “America in Islam” (Washington, DC: Hudson Institute, Spring 2004), www.hudson.org/files/publications/america_in_islam.pdf; Khaled Abou El Fadl, Testimony before the 9/11 Commission, Dec. 6, 2003; John Tirman, ed., *The Maze of Fear, Security and Migration after 9/11* (New York: New Press, 2004); Enseng Ho, “Empire Through Diasporic Eyes” (Harvard University Department of Anthropology, n.d.), 17-44; Spencer Ackerman, “Why American Muslims Haven’t Turned to Terrorism,” *The New Republic Online* (Dec. 12, 2005), <http://www.tnr.com/doc.mhtml?i=20051212&s=ackerman121205>; Peter Skerry, “Political Islam in the United States and Europe” in *Political Islam: Challenges for U.S. Policy*, ed. Dick Clark (Aspen Institute Congressional Program, 2003), http://www.brookings.edu/gs/skerry_islam.pdf.

10 Office of Homeland Security, *National Strategy for Homeland Security*, July 2002, vii-xiii, http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

11 John Kane and April Wald, “Identifying the Links Between White Collar Crime and Terrorism,” Grant No. 2003-IJ-CX-1018 (US Department of Justice, National Institute of Justice, Office of Justice Programs, Sept. 2004), <http://www.ncjrs.org/pdffiles1/nij/grants/209520.pdf>. This analysis of cases effectively alerts other prosecutors to options for charging suspected terrorists with mobility-related and other crimes. But it raises additional questions relevant to assessing the impact of mobility factors in counterterrorism. At the investigative level, it would be useful to know what percentage of cases involved travel documents or other mobility factors triggering detection of the terrorist *in the first instance*. At the level of prosecution, it would be helpful to understand whether immigration law related charges were used as a substitute for or to bolster direct terrorism charges based on other evidence or classified information. Finally, the study does not detail the miscarriages of justice and infringement of civil liberties and human rights that may have occurred. Charging terrorists with criminal immigration offenses is often a tactic of choice for prosecutors because the government can achieve disruption of terrorist activity without having to disclose classified information to charge the individual. Under such circumstances, procedural due process is particularly vulnerable, and groups may be targeted disproportionately to their involvement in illegal activity. To make a more complete assessment of the cases, a study would have to track the case from initial lead through the investigation, to charging, decision, penalty, and appeal outcomes. Nevertheless, the study’s documentation of the widespread use of travel document and immigration-related charges in terrorism-related prosecutions is suggestive of the major significance of the need for transnational mobility as a vulnerability to be exploited.

12 For an analysis of an overlapping group of 119 cases, see the Center on Law and Security, “Terrorist Trials: A Report Card” (New York University Law School, Feb. 2005), <http://www.law.nyu.edu/centers/lawsecurity/publications/terroristtrialreportcard.pdf>.

13 See, e.g. Migration Policy Institute, “Immigration and National Security,” Background Paper (Washington, DC: Migration Policy Institute, Sept. 28, 2001), http://www.migrationpolicy.org/files/928_backgroundunder.pdf. While focusing primarily on security improvements in legal entry channels, this paper also envisioned eventual US-Canadian harmonization of visa regimes and coordination of asylum policies that respond to mutual security needs in North America. The Bush Administration has taken steps in this general direction, most recently by establishing a “Security and Prosperity Partnership of North America.” See US Department of State, “Security and Prosperity Partnership of North America,” Fact Sheet, March 23, 2005, <http://fpc.state.gov/fpc/43780.htm>. The harmonization vision, however, is radical relative to progress in the trination dialogue.

14 The knowledge model is adapted from a similar model developed for the Bureau of Alcohol, Tobacco, Firearms and Explosives, Department of Justice, as a basis for describing how firearms trafficking intelligence systems support investigations, prosecutions, regulatory

and other actions. See Glenn Pierce and Roberta Griffith, "Firearms Tracking Intelligence Systems: the Southern California Regional Crime Gun Center," (Boston, MA: Northeastern University, College of Criminal Justice, 2005).

15 E.g. International Crisis Group, "Counter-Terrorism in Somalia: Losing Hearts and Minds?" in Africa Report (London, ICG, July 11, 2005); "Islamist militant faces French probe for assisting Iraq jihad volunteers," Agence France-Presse (May 13, 2005) FBIS EUP20050513950114 (France); Karlsruhe Federal Prosecutor General's Office, "Germany: Three assumed Ansar Al-Islam supporters arrested, premises searched," (January 14, 2005) FBIS EUP20050615072002 (Germany); "German police conduct raids in five states against Islamic extremists," Associated Press (January 12, 2005); "German BND sees increasing cooperation between Islamists, organized crime," Munich *Suddeutsche Zeitung* (October 9, 2004) FBIS, EUP20041009000117 (Germany); "French authorities arrest alleged Islamist militant sought by Italy" Agence France-Presse (July 13, 2005) FBIS EUP20050713950032 (Italy); "Arrest of 16 terrorist suspects in Spain," *Madrid RNE Radio 1* (June 15, 2005) FBIS EUP20050615950021 (Spain). See also Robert S. Leiken, "Europe's Angry Muslims," *Foreign Affairs* (July/August 2005).

16 Alisa Tang, "Thailand emerges as fake passport capital," Associated Press, September 8, 2005.

17 *National Strategy for Homeland Security* (see n. 10), viii, 19.

18 Rob Buschmann, "Risk Assessment in the President's National Strategy for Homeland Security," (Congressional Research Service, 2002).

19 For a discussion of reverse engineering in organizations, see Darrel S. Raynor, "Reengineering: Information Systems and Business," (Austin, TX: Data Analysis and Results, Inc., May 27, 1993), <http://www.dataanalysis.com/dataanalysis/RRpts/FTRNG053.htm>.

20 A survey of the variety of illicit networks trading in goods and services permeating the global economy is presented in Moises Naim, *Illicit: How Smugglers, Traffickers, and Copycats Are Hijacking the Global Economy* (New York: Doubleday, 2005); see also Moises Naim, "The Five Wars of Globalization," *Foreign Policy* (January-February 2003), 29-36.

21 Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, Section 7202.

22 A centralized effort to focus resources against human smuggling organizations particularly accessible to terrorist organizations is alluded to in news reports. See Shaun Waterman, "Alien smugglers could have been deported ten years ago," United Press International, Dec. 13, 2005.

23 David M. Kennedy, *Reconsidering Deterrence*, manuscript (July 2004); "Pulling Levers: Chronic Offenders, High-crime Settings, and a Theory of Prevention" *Valparaiso University Law Review* (1997); "Pulling Levers: Getting Deterrence Right," *National Institute of Justice Journal* (July 1998).

24 See Rey Koslowski, "Possible steps towards an international regime for mobility and security," *Global Migration Perspectives*, No. 8 (Geneva: Commission on International Migration, Oct. 2004). In addition to considering the role of security in migration-related agreements as this paper contemplates, it would be useful to assess progress in addressing and acting on terrorist mobility in existing United Nations and regional terrorism instruments.

25 Khaled Abou El Fadl, Testimony before the 9/11 Commission, December 6, 2003.

26 Dana Priest, "Wrongful Imprisonment: Anatomy of a CIA Mistake," *The Washington Post*, December 4, 2005.

27 Dana Priest, "Foreign Network at Front of CIA's Terror Fight, Joint Facilities in Two Dozen Countries Account for Bulk of Agency's Post-9/11 Successes" *The Washington Post*, Nov. 21, 2005; Dana Priest, "Help From France Key in Covert Operations; Paris' 'Alliance Base' Targets Terrorists," *The Washington Post*, July 2, 2005.

28 Vivid depictions of new battlefield information capabilities abound. See e.g. *NOVA: Battle Plan Under Fire* (PBS Network, May 4, 2004).

29 *National Strategy for Homeland Security* (see n. 10), 22.

30 This can be seen, for instance, in the most recent announcement by the Departments of State and Homeland Security of modifications to visa and entry processing – the real-time access to immigration and other information by visa offices, and the planned progression to paperless visa processing, a global enrollment network, and harmonized screening standards, together with the establishment of a virtual clearinghouse for screening information that ought to permit centralized analysis. Department of Homeland Security, "Secure Borders and Open Doors in the Information Age," Fact Sheet, January 17, 2006, http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0838.xml.

31 Jess T. Ford, "Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts" (US Government Accountability Office, GAO-05-853T, May 2005), 11. This report recommends the establishment of an electronic library.

32 *National Strategy for Homeland Security* (see n. 10), 57.

33 The US-VISIT program and its considerable challenges are described in Rey Koslowski, *Real Challenges for Virtual Borders: The Implementation of US-VISIT* (Washington, DC: Migration Policy Institute, June 2005).

34 "Real Challenges for Virtual Borders" (see n. 33).

35 See Department of Homeland Security, "Select Homeland Security Accomplishments for 2005," Press Release, Dec. 20, 2005, www.dhs.gov/dhspublic.

36 Homeland Security Presidential Directive 11 directed planning for comprehensive terrorist-related screening procedures. The 9/11 Commission recommended establishment of a network of screening points. *The 9/11 Commission Report* (see n. 1), 387.

37 See Faye Bowers, "Why Mexico helps US fight terror," the *Christian Science Monitor*, January 26, 2006.

38 *National Strategy for Homeland Security* (see n. 10), 22.

39 *The 9/11 Commission Report* (see n. 1), 390.

40 Department of Homeland Security, "Secure Border Initiative," Fact Sheet, November 8, 2005. The overall vision includes more agents to patrol borders, secure ports of entry, and enforce immigration laws; expanded detention and removal powers to end "catch and release" practices; a comprehensive and systematic upgrading of technology used in controlling the border, including increased manned aerial assets, expanded use of UAVs, and new detection technology; increased investment in infrastructure improvements at the border, providing additional physical security to reduce illegal border crossings; and greatly increased interior enforcement of our immigration laws.

41 Aspects of such a plan are discussed in Michael E. O'Hanlon et al., *Protecting the American Homeland, One Year On*, (Washington, DC: Brookings Institution, 2003), 13-35. The analysis includes a mix of steps encompassing both border and immigration management involving legal channels and perimeter defense involving illegal channels.

42 Oscar Becerra, "Mexican people-smuggling trade worth billions," *Jane's Intelligence Review*, December 2004.

43 Shaun Waterman, "Canada fears a new generation of terrorists," UPO, Inc., May 13, 2005, <http://www.upo.com/view.cfm?StoryID=20050512-075511-9678r>; Beth Duff-Brown and Pauline Arrillaga, "U.S.-Canada Border Leaves Many Jittery," Associated Press, July 4, 2005, <http://wireserve.wired.com>.

44 In discussing US immigration policy, this report generally avoids using either the phrases "irregular" or "illegal" alien or migration, in order to deemphasize the focus on the migration status of individuals or groups and instead highlight the problem of terrorist exploitation of legal or illegal entry and residence channels. Within the United States, immigration laws are clearly being broken on a large scale, and many migrants are here illegally, making them illegal aliens who have engaged in illegal migration. Within the context of dialogue among states, the most recently proposed term for "a variety of different phenomena involving people who enter or remain in a country of which they are not a citizen in breach of national laws" is "irregular migration." The rationale for this terminology is described in the report "Migration in an inter-connected world: New directions for action," Report of the Global Commission on International Migration (GCIM), October 2005. The GCIM is an independent body sponsored by a core group of nineteen United Nations Member States not including the United States. See also Khalid Kaser, *Irregular Migration, State Security and Human Security*, GCIM, September 2005.

45 Department of Justice and Department of Homeland Security, "Fusion Center Guidelines, Law Enforcement Intelligence Component," July 2005 (Version 1); Homeland Security Advisory Council, "Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion," April 28, 2005; Homeland Security Advisory Council, "Intelligence and Information Sharing Initiative, Final Report," December 2004.

46 A version of this recommendation is included in Gary Hart and Warren B. Rudman, *America—Still In Danger, Still Unprepared* (Washington, DC: Council on Foreign Relations, Oct. 2002).

47 See e.g. Dan Benjamin and Steven Simon, *The Next Attack* (New York: Times Books, 2005), 114-18, 120-22.

48 The observation has been made that there is little good social science on the American Muslim community. *The Next Attack* (see n. 47).

49 See Dorian Zumel-Sicat, "RP Cops aware of long-term rightwing, Muslim connection," *The Manila Times*, April 26, 2002; Kenneth R. Timmerman, "Revealed—Iraq Was Involved in the Oklahoma City Bombing," *Insight Magazine*, April 23, 2002, <http://www.rense.com/general24/rev.htm>.

50 *America the Vulnerable* (see n. 1).

51 Walter Pincus, "Pentagon's Intelligence Authority Widens, Fact Sheet Details Secretive Agency's Growth From Focus on Policy to Counterterrorism," *The Washington Post*, Dec. 19, 2005 (describing the three year old Counterintelligence Field Activity (CIFA)).

52 Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, Section 7202.

53 Although post-9/11 legislation shifted responsibility for visa policy from the Department of State (DOS) to the Department of Homeland Security (DHS), as a practical matter DOS and its counterterrorism coordinator must remain responsible for the terrorism-related integration of consular affairs with a range of closely related DOS functions—the Diplomatic Security Bureau's visa and passport fraud authorities, international law enforcement matters, the

Economic Bureau's anticorruption policy role, and International Organizations with its focus on multilateral organization agendas and treaties, among other functions. Congress's decision to assign ICE investigators as "visa security officers" to increase visa officer access to law enforcement information and techniques instead of enhancing and assigning officers of the Department of State's own Diplomatic Security investigative force is puzzling, especially since Diplomatic Security officers are trained to operate overseas.

54 John Brennan, "Is This Intelligence? We Added Players But Lost Control of the Ball," *The Washington Post*, November 20, 2005. Brennan comments that, "While the 9/11 Commission called for a national counterterrorism center to have primary responsibility for terrorism analysis and strategic operational planning, the WMD commission called for a small national counterproliferation center to serve a staff function and orchestrate the work of others . . . now the intelligence community is trying to figure out how to hard-wire two very dissimilar centers." He recommends that the director of national intelligence appoint a small team of experienced experts to reconcile these two models. It is not clear why different models might not be correct for different problems, but in any case the wait for structural modifications should not delay development of a terrorist mobility strategy directly called for by statute and the exercise of coordinating management to implement in implementing it.

55 Luis Redueles, Manuel Mariasca, "Los jefes Al Qaeda usan pasaportes españoles."

56 Henry A. Crumpton, "Intelligence and Homeland Defense," in *Transforming US Intelligence*, ed. Jennifer E. Sims and Burton Gerber, 200 (Washington, DC: Georgetown University Press, 2005).

57 "Special Report, Financing Terrorism, Looking in the Wrong Places, Hindering flows across international financial networks is costly and does not stop terrorists' primary activity," *The Economist*, October 22, 2005. In response to such criticism, there is a need for the counterterrorism and business communities to use hands-on knowledge of systems and trends to redesign techniques to make terrorist finance detection more cost-effective.

58 How the multiple US strategies relate to one another within our constitutional framework is described in the *National Strategy for Homeland Security*, (see n. 10), 5.

59 The White House, *The National Security Strategy of the United States of America*, September 2002, 5, 6, 31.

60 *National Strategy for Homeland Security* (see n. 10).

61 *National Strategy for Combating Terrorism*, February 2003, 26, 17, 18-19, 20, 26, 22, 7.

62 Department of Defense, *Strategy for Homeland Defense and Civil Support*, June 2005, 1-2, 6, 15.

63 Department of Defense, *National Military Strategic Plan for the War on Terrorism*, February 2006, 5 (nine elements), 6-7 (elements of study), 9 (strategic guidance flowchart), 16-17 (movement). <http://www.defenselink.mil/qdr/docs/2005-01-25-Strategic-Plan.pdf>.

ACKNOWLEDGEMENTS

The author would like to thank John Brennan, Mark A.R. Kleiman, Douglas J. MacEachin, Doris Meissner, and Glenn Pierce for their helpful comments and Demetrios G. Papademetriou and Chris Kojm for their encouragement. Any errors are my own.

ABOUT THE AUTHOR

Susan Ginsburg is an independent consultant and policy analyst. She served as a Senior Counsel for the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), and Team Leader for its group examining how terrorists were able to enter the United States. Previously, she served as Chief of Staff and Senior Advisor to the Under Secretary for Enforcement at the Department of the Treasury from 1994-2001. She served as Special Assistant at the Department of States Office of International Narcotics Matters from 1979-1981. A lawyer, she has practiced law as a civil litigator and served as law clerk to Judge A. Leon Higginbotham of the Third Circuit Court of Appeals. She has also worked as a Legislative Assistant in the House of Representatives.

This report was commissioned as part of MPI's Independent Task Force on Immigration and America's Future. The task force, a bipartisan panel of prominent leaders from key sectors concerned with immigration, aims to generate sound information and workable policy ideas. Former Senator Spencer Abraham (R-MI) and former Congressman Lee Hamilton (D-IN) serve as co-chairs, and the task force's work is directed by MPI Senior Fellow Doris Meissner, the former commissioner of the Immigration and Naturalization Service. MPI's partner institutions in the project are Manhattan Institute and the Woodrow Wilson International Center for Scholars.

The report examines the connection between counterterrorism and immigration reform. While public discourse tends to equate blocking terrorists' ability to travel with reforming the immigration system, author Susan Ginsburg argues that terrorist mobility confronts us with a set of problems distinct from, although clearly linked to, the phenomenon of global migration and the problem of controlling immigration. She proposes that constraining terrorist mobility be adopted formally as an operational counterterrorism strategy, analogous to the approach to terrorist finance. Her report sets forth a series of interwoven measures that the United States and its security partners can use to simultaneously exploit terrorist mobility and reduce the country's vulnerability. Ms. Ginsburg cautions that US immigration reform, especially insofar as it focuses heavily on preventing migration through illegal channels from Mexico, cannot be seen as a substitute for a prominent, integrated US strategy that can counter a terrorist mobility threat from multiple directions.

For more information about the Independent Task Force on Immigration and America's Future, please visit www.migrationpolicy.org.



mpi
MIGRATION POLICY INSTITUTE

1400 16th Street NW
Suite 300
Washington, DC 20036

202 266 1940
202 266 1900 fax

www.migrationpolicy.org