TESTIMONY

Border Security and the Terrorist Threat

K. JACK RILEY

CT-266

August 2006

Testimony presented to the House Homeland Security Committee, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, Subcommittee on Emergency Preparedness, Science, and Technology on August 8, 2006

Published 2006 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Dr. Jack Riley[1]
The RAND Corporation

Border Security and the Terrorist Threat

Before the Committee on Homeland Security
Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity
Subcommittee on Emergency Preparedness, Science, and Technology
United State House of Representatives

August 8, 2006

Introduction

There are few homeland security challenges as daunting—and urgent—as securing the nation's borders. Every day, nearly 20,000 cargo containers enter U.S. ports and every year, nearly 90 million passengers land at the more than 100 international airports scattered across the country. Add to the sea and air borders the thousands of miles of land borders shared with Canada and Mexico and the importance of those land borders to trade and tourism, and the magnitude of the challenge becomes abundantly clear. These statistics should also make clear how security can interact with commerce and economic activity. Decisions about security at the border have the potential to affect the livelihood of millions of Americans and a significant portion of the U.S. economy.

If there is an overarching theme to this testimony, it is that we have woefully underinvested in developing, evaluating, and refining a comprehensive and integrated border security strategy. We have invested in numerous border security programs and initiatives but the impacts and cost-effectiveness of virtually all of these initiatives is poorly understood. We are virtually flying blind on a topic of critical national importance.

Now that I have raised the alarm, let me turn to a review of one key instance that provides important insights for contemporary border security practices.

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

The Millennium Bomber

On December 14, 1999, Ahmed Ressam was captured near the U.S.-Canadian border by sharp-eyed border security personnel.[2] Ressam, trained in terrorist attack methods, was headed to Los Angeles with plans to detonate multiple bombs simultaneously at Los Angeles International Airport. His intent to conduct the attack on New Year's Eve 1999 earned him the sobriquet "the millennium bomber." As lessons in border security go, it is hard to point to one that more clearly illustrates the complexities of border control than the Ahmed Ressam case.

Ressam is Algerian by birth and tried to enter Canada in 1994 on a forged passport. His passport aroused suspicions and, fearing that he would not be able to gain entry, Ressam claimed political asylum on the basis of alleged political persecution in Algeria. He became one of approximately 30,000 people seeking political asylum in Canada that year. He was admitted pending the outcome of an asylum hearing that would determine the eligibility of his claim. Ressam was not placed in custody despite several warning signs that raised doubts as to the legitimacy of his claim and his suitability for prehearing release, including his own statements that he was falsely accused of arms trafficking in his home country.[3] Ressam skipped the hearing scheduled for June 1995. A warrant was issued for his arrest but he avoided deportation by obtaining false documentation (including a baptismal certificate and passport) under the identity "Benni Noris." Authorities were unaware of his new alias but were actively looking for Ahmed Ressam during this period. Ressam was able to use the false identity to travel to Afghanistan in 1998 for terrorist training.

On December 14, 1999, U.S. immigration agents operating in Victoria, British Columbia, allowed Ressam to board a ferry that took him to Port Angeles, Washington. In Port Angeles, outside Seattle, Ressam hesitated to answer questions posed by a customs agent. He was asked for identification and, panicked, attempted to flee. It was at this point that U.S. authorities took Ressam into custody. A search of his car revealed materials, concealed in the trunk, to make bombs.

---

[2] For a detailed accounting of the Ahmed Ressam case and its implications, see "Trail of a Terrorist" (Terence McKenna, WGBH Educational Foundation and Canadian Broadcasting Corporation, 2001; online at http://www.pbs/org/wgbh/pages/frontline/shows/trail as of August 2, 2006)..See also *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, (National Commission on Terrorist Attacks upon the United States, New York: Norton, 2004; online at http://www.gpoaccess.gov/911/index.html as of August 2, 2006), pp. 172–184.

[3] A falsified passport in and of itself may not be sufficient to merit preventive detention. Indeed, experience has shown that many legitimate asylum claimants use falsified travel documents to escape their conditions of persecution.

The Ressam incident reveals several key points about border security:

- **Technology is not a substitute for trained, professional security personnel.** It was not technology that caught Ahmed Ressam in 1999. It was good, old-fashioned security experience that resulted in Ressam's capture and the disruption of the attack.
- **False documents are the currency of the terrorist trade.** Ressam was able to falsify a passport that got him on a plane to Canada. Once in Canada, he was able to create another passport that allowed him to travel to Afghanistan, where he was trained in one of Osama bin Laden's terrorist camps. Perhaps most important, he was able to create a new identity that allowed him to avoid being arrested while the authorities sought "Ahmed Ressam."
- **The border threat is not just a southern phenomenon; there is threat from the north.** As early as 1998, Canada's Special Senate Committee on Security and Intelligence labeled Canada "a 'venue of opportunity' for terrorist groups: a place where they may raise funds, purchase arms, and conduct other activities to support their organizations and their terrorist activities elsewhere. Most of the major international terrorist organizations have a presence in Canada. Our geographic location also makes Canada a favorite conduit for terrorists wishing to enter the United States, which remains the principal target for terrorist attacks worldwide."[4] More recently, the Canadian Security Intelligence Service acknowledged in its 2004–2005 annual report that "[a] relatively large number of terrorist groups [is] known to be operating in Canada, engaged in fundraising, procuring materials, spreading propaganda, recruiting followers and conducting other activities."[5]
- **Our allies face many of the same border security problems as the United States faces.** In 1994, the year that Ressam entered Canada, there were some differences in how the United States and Canada handled asylum claims. However, Canadian and U.S. officials confronted many similar issues at that time, including a shortage of personnel to patrol the vast physical borders, an inability to ensure that immigrants and asylum-seeking individuals complied with the terms of their entry, and no reliable system for ensuring that international travelers were traveling with valid passports. U.S. border security is thus, to some extent, a hemispheric, if not international, issue.

---

[4] *The Report of the Special Senate Committee on Security and Intelligence* (The Honourable William M. Kelly, Chairman, Ottawa: Special Senate Committee on Security and Intelligence, January 1999).

[5] *Public Report 2004–2005* (Canadian Security Intelligence Service, Ottawa: Public Works and Government, 2006; online at http://www.csis-scrs.gc.ca/en/publications/annual_report/2004/report2004_e.pdf as of August 2, 2006).

Principles of Effective Border Security

Where Ahmed Ressam failed to exploit the borders in his disrupted effort of 1999, the 9/11 terrorists succeeded. The 9/11 hijackers exploited many of the same vulnerabilities that Ressam attempted to exploit, including use of fraudulent travel documents and capitalizing on the laxity in our detention and deportation capabilities. But the 9/11 attacks also revealed additional border security vulnerabilities. Examples of additional border security weaknesses included the lack of physical security on aircraft, the weaknesses of the command and control system of the civilian air network, and the insufficiency of intelligence coordination within and across agencies.[6]

In the immediate aftermath of 9/11, officials moved quickly to close major border security gaps. The key steps in these efforts are described in subsequent sections of this testimony. Before discussing specific steps taken to improve border security, it is appropriate to review some overarching principles about effective border security that have emerged since 9/11. In general terms, an effective border security strategy consists of operational control over people and weapons. It must exist at our land borders, ports and airports. It must ensure effective communications among the myriad agencies charged with regulating the commerce and security at the border. And it must provide an effective deterrent that raises the costs to, and increases the visibility of, those that seek to attack our society.

There are three critical principles that underpin border security.

- **There is no single programmatic fix.** Border security will be achieved through a network of mutually reinforcing, and to some extent redundant, layers of defenses. There is no easy solution. Border security is a long-term challenge that will always be marked by terrorists' efforts to identify and exploit the weakest link. As a consequence, we need to consider not just the effects of individual programs, but the interaction effects of multiple programs.
- **Border protection begins far from our shores, airports, and crossing points.** Border security is more effective when we have programs that reach toward the points of origin, rather than simply relying on defending the fixed points of the border. A wide variety of programs fall into this category and should be considered part of the border security effort, including intelligence efforts to monitor the movements of suspected terrorists,

[6] *The 9/11 Commission Report* provides perhaps the most authoritative and comprehensive review weaknesses that were exploited.

efforts to reducing trafficking in stolen passports and make legitimate passports more tamperproof, and efforts to obtain advance information and conduct advance screening of passengers and cargo entering the United States.

- **We can reduce the volume of work and the magnitude of the task through more effective use of information and technology.** In some circumstances, we can use information and technology to help "profile out" and allow trusted passengers and cargo to circumvent routine inspection. That is, we can identify pools of passengers and cargo that do not merit attention beyond random checks and screening because they are trustworthy, have been verified by reliable allies, or because the content of their conveyance is known with a high degree of certainty. When low-risk passengers and cargo are profiled out, resources can be focused on remaining, and potentially more troubling, risks. A related concept is the need for faster, less expensive, and more reliable technologies. These technologies, which have uses such as screening cargo, detecting unconventional weapons, and monitoring the border, are vital to our ability to provide for homeland security.

Border Security Improvements Since 9/11

Since the terrorist attacks of September 11, substantial progress on border security has been made. Improvements that cut across border segments are discussed first, followed by additional improvements specific to each border segment.

Cross-Cutting Security Measures

Several post-9/11 security measures have applicability to more than one segment of the border. These measures are reviewed briefly here, followed by a review of key border security initiatives by border segment.

REAL ID Act. In May 2005, Congress passed the REAL ID Act.[7] The Act requires that, by 2008, state driver's licenses meet minimum security requirements. To receive a license, an individual will have to present photo identification, documentation of the date of birth, proof of social security number (or of ineligibility for such number) and documentation showing the applicant's name and address of primary residence. State IDs that do not comply with this framework may not be

[7] "Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005 (Enrolled as Agreed to or Passed by Both House and Senate)," H. R. 1268, Division B, 2005.

acceptable for federal purposes such as boarding a plane. A data network will link all 50 states so that there are reduced opportunities for cross-state fraud. The REAL ID Act lets states offer illegal immigrants a “driving only” license to applicants who are unable to prove their legal status in the United States. Such a license would be marked as not being valid for the purpose of identification. If the act is implemented as designed, it should help cut down on the availability of false identification.

Passport and Visa Improvements. Since 9/11, numerous changes to the process by which foreigners travel to the United States have occurred. The most important of these changes include the development of the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program and the strengthening of passport and visa requirements for travel to the United States. Under US-VISIT, certain non-U.S. travelers to the United States have their two index fingers digitally scanned and a digital photograph taken at the U.S. port of entry. The fingerprints are then instantly checked against criminal information databases. Eventually, travelers are expected to be able to use US-VISIT as they exit the United States. Once in place, this system will help U.S. officials know with greater certainty when individuals remain in the United States longer than their visas permit.

Travelers from visa waiver program (VWP) countries must now participate in US-VISIT. Under the VWP, travelers from 27 countries (mostly European) are not required to obtain a visa when traveling to the United States for periods of 90 days or less. Countries participating in the VWP must issue their citizens machine-readable passports that contain biometric data.

Persons traveling from non-VWP countries must obtain a visa. In the aftermath of 9/11, the visa review process has been tightened significantly. Visas for travel to the United States now include biometric markers of fingerprints and a digital rendering of the face. To obtain the initial biometric information, visa applicants are required to submit to an in-person interview with a consular officer. In-person interviews may also be required for people traveling from certain countries even after biometric visa data is on record.

As a consequence of all of these changes, it is now more difficult for terrorists to enter the country using fraudulent documents through official points of entry. Indeed, since US-VISIT biometric processing was initiated on January 5, 2004, more than 1,000 individuals have been arrested or otherwise denied admission at U.S. borders. The concern, however, is that the success at the legal points of entry may force more efforts at crossing between official ports of entry.

Air Transportation

Given the nature of the 9/11 attacks, it is not surprising that many improvements in air transportation security have been implemented. Among the most notable accomplishments are the following:

- strengthening the security of cockpit doors to prevent intrusion
- implementing a system to screen checked luggage for explosives and other dangerous goods
- expanding armed patrolling of flights through the Federal Air Marshal Service.

These are among the many steps that have been taken to reduce the likelihood of future hijackings.

Land Border Crossings

Land border crossings remain a vital component of our national economy. At the same time, they are difficult to control, given that there are more than 6,000 miles of shared borders between the United States, Mexico, and Canada. Some of the notable security steps taken since 9/11 on the land border front include the following:

- the creation of fast lanes of various sorts to facilitate the movement of commerce and profile out trusted shipping sources. Examples include the opening of multiple NEXUS lanes between the United States and Canada and the development of a similar program, Free and Secure Trade (FAST), that addresses commercial shipping.[8]
- The development, under the Secure Border Initiative, of a plan to upgrade the technology used border control, including expanding the use of occupied and unoccupied aerial assets and accelerating the deployment of detection technology and sensors.
- Deployment of more personnel along the border. Since 9/11, the border patrol has increased by approximately 2,000 officers in size, and an additional 1,000 new hires are planned.

[8] At the U.S. border with Mexico, the Secure Electronic Network for Travelers Rapid Inspection (SENTRI) program, similar to NEXUS, facilitates noncommercial border crossings.

Shipping and Ports

After 9/11, customs and border personnel moved quickly to secure the commerce flowing through our nation's ports. Among the more important measures:

- the development of the Customs-Trade Partnership Against Terrorism (C-TPAT), under which firms voluntarily ensure the integrity of the security processes in exchange for priority processing, reductions in the number of security checks, and other steps that facilitate the movement of goods. C-TPAT has been an important avenue for engaging the private sector in supply chain security.
- the initiation of the Container Security Initiative (CSI), under which border personnel try to identify high-risk containers, prescreen and evaluate containers before they arrive in the United States, and develop new generations of containers that offer additional security. CSI's significance rests in the fact that it initiates the security process long before the cargo reaches U.S. shores.

In addition, the Department of Homeland Security (DHS) has given out numerous grants to facilitate improvements in the physical security of ports around the country. Presently, DHS is screening about 50 percent of the containers arriving by ship for radiological and nuclear material using radiation portal monitors. And approximately 80 to 90 percent of the containers at land borders are being screened. Although this cargo screening effort is significant, it is important to point out that the cost-effectiveness of the approach has not been established.

Remaining Border Security Challenges

Though substantial progress has been made since 9/11 in border security, substantial challenges remain.

Toward a National Strategy

H.R. 4437 calls for the development of a National Border Control Strategy (NBCS). This call is welcome and long overdue. Border security is sufficiently complicated and vital to homeland security that establishing a periodic NBCS review process may be appropriate. For example, the Department of Defense conducts a review every four years (the Quadrennial Defense Review or QDR) to assess strategy, "force structure, force modernization plans, infrastructure, budget plans, and other elements of the defense program and policies of the United States with a view toward

determining and expressing the defense strategy of the United States and establishing a defense program for the next 20 years."[9] This type of periodic review is also critical for dealing with changes in the level or nature of the threat – whether that is numbers of people crossing the border, how they are trying to penetrate, or the techniques used.

In late 2005, the President and Secretary Chertoff announced the creation of the Secure Border Initiative (SBI). This initiative, which increases the number of border personnel and their enforcement activities, expands detention and removal capabilities and other infrastructure, and invests in border-related technologies, is a solid start. SBI is a building block for the development of the NBCS. By itself, however, the SBI does not address border security in sufficient depth and breadth to constitute a strategy.

An effective NBCS will include the following:

- **The establishment of concrete benchmarks and performance metrics.** Concrete benchmarks and performance metrics will allow realistic and systematic appraisal of the tradeoffs across various programmatic choices and provide guidance on where to invest additional funds. Without these benchmarks, we will not know which programs work and which ones need adjustment. As homeland security resources become scarcer, it becomes increasingly important to invest in programs that fill critical security gaps in a cost-effective manner.
- **The development of a comprehensive border technology roadmap.** Most of our technology needs can be summed up with the statement, "faster, cheaper, more reliable." These characteristics, however, must be linked to policies and to a careful consideration of the problems we are trying to solve. When there is a pressing need for security, there can be an incentive to invest in any—or all—apparent technological solutions, regardless of the potential payoff. For example, there were early calls to establish a missile defense system for the passenger air travel system, though subsequent analyses demonstrated that the public dollars could be better spent on other security measures.[10] It is important

---

[9] 10 U.S.C. 118.

[10] *Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat* (James S. Chow, James Chiesa, Paul Dreyer, Mel Eisman, Theodore W. Karasik, Joel Kvitky, Sherrill Lingel, David Ochmanek, and Chad Shirley, Santa Monica, Calif.: RAND Corporation, OP-106-RC, 2005; online at http://www.rand.org/pubs/occasional_papers/OP106 as of August 2, 2006). See also *A Decision Analysis to Evaluate the Cost-Effectiveness of MANPADS Countermeasures*, (Detlof von Winterfeldt and Terrence M. O'Sullivan, Center for Risk and Economic Analysis of Terrorism Events (CREATE), University of Southern California, October 16, 2005; draft online at http://www.usc.edu/dept/create/events/2005_01_31/von%20Winterfeldt%20and%20O'Sullivan%2011-22-05.pdf as of August 2, 2006).

to structure the spending pattern to invest in technologies that will yield high payoffs, address mission-relevant functions, and provide essential capabilities and over a policy-relevant time horizon.

- **The development of a border security force plan.** The border security problem is dynamic. As a consequence, we need personnel that have the requisite skills to combat the current threat, but that also are capable of responding to new and emerging challenges. In the same way that military institutions conduct force mix studies and attempt to project their personnel needs in different skill categories, so too must our border security forces identify the critical skills—both leadership and rank-and-file—that it needs. These skill needs assessments can then be linked to needs in training, recruitment, retention and other critical areas of force management.
- **The creation of plans for managing the border during crises.** Odds are, at some point, our border security measures will fail. An overlooked but important aspect of border security is how it will function after a security breach. For example, after an attack using the supply chain and the ports, presumably the port system would at least be temporarily shut down. Under what conditions do we reopen the ports?

Illegal Immigration and Visa Overstays

As documented by the 9/11 Commission, all of the 9/11 terrorists had at least one form of acceptable identification, such as a passport issued by a foreign country or a U.S. driver's license. In many cases, these documents were obtained fraudulently. Nevertheless, their possession of these documents facilitated their travel into and out of the United States and facilitated their movement around the United States. Their ability to acquire fraudulent documents made it more difficult to locate and deport those 9/11 hijackers who had overstayed their visas. Indeed, at any given moment, more than 400,000 individuals in the United States are living here in violation of lawful deportation orders.

In addition to the roughly half-million individuals lawfully adjudicated for deportation, an estimated 10 million simply entered the United States illegally without any paperwork. Many in this pool are drawn by the availability of jobs and other opportunities in the United States.

The high volume of illegal overstays in and illegal entries into the United States constitutes a substantial security risk in several ways. First, it spreads the attention and limited resources of border enforcement across a very large base. Second, it creates a substantial shadow economy in which terrorists and other criminals can hide and a smuggling and transport infrastructure they

can exploit. Third, it demonstrates to terrorists how easy illegal entry is. A vital part of security is thus figuring out how to deter illegal visa overstays and immigration.

No existing program or combination of existing programs seems likely to cut down significantly on either of these problems, especially illegal immigration. Improved passport security and visa security make it more difficult for undesirable aliens to obtain permission to enter the United States. Though it is by no means certain, these programs may help shift the terrorists' attention to smuggling personnel over the long and difficult-to-regulate land border, rather than through airports and other formal ports of entry. And, once in, such individuals will face little risk of apprehension and deportation. Similarly, the REAL ID Act will do little to break the link between illegal immigration and employment. Under current procedures, which are passive, employers are only required to make a prospective employee provide identification. The REAL ID Act will not help in this case, because employers do not have the equipment or expertise to validate the identification. In addition, it seems clear that we will not be able to create the amount of detention capacity to provide a deterrent.

Instead, it should be a high priority to develop a program that helps reduce the incentive to enter the United States illegally. One possibility would be a program that requires employers to instantly check non-U.S. citizens against eligibility lists. H.R. 4437 provides one such system.[11] Congress would need to decide who is put on the eligibility lists—for example, immigrants currently residing in the United States who entered illegally or only legal residents and aliens. If properly implemented, such a system could help reduce the incentive to immigrate illegally. In turn, enforcement officials could then concentrate resources on controlling the smaller flows of individuals who are illegally crossing the borders. Such a system, however, presents daunting operational challenges and the costs and benefits of the approach have yet to be clearly assessed. That said, it should be a high priority to develop a program that helps reduce the incentive to enter the United States illegally.

Air Transportation

Screening passengers for explosives. Despite improvements in screening at airports, we lag in our ability to detect explosives on passengers. Richard Reid, the infamous shoe bomber, smuggled a bomb on board a flight from Paris to Miami and was thwarted only when he

[11] A similar system is currently being tested with criminal aliens to determine their eligibility for deportation as they are being released from U.S. jails.

attempted to ignite the fuse in the passenger cabin. In August 2004, Chechen terrorists brought down two Russian passenger aircraft when suicide terrorists ignited bombs.[12] Traditional screening methods are unreliable in that explosives may be disassembled to resemble innocuous household objects or the explosives may not be detectable by in-baggage screening equipment. Swabbing baggage for traces of explosives is more effective, though such methods are used on only a small portion of bags passing through screening. The Transportation Security Administration (TSA) has begun experimentation with explosive detection portals that send strong puffs of air through a chamber in which the passenger stands. The resultant air samples are then rapidly tested for traces of explosives. These portals, and similar methods, are potentially important additions to passenger security, though long-term effectiveness, cost of operation, and impact on passenger throughput are not fully known at this point.

Screening cargo for explosives. More than 20 percent of the cargo that moves by airplane is thought to be transported on passenger planes. Passenger flights are thus vulnerable to the terrorists' ability to smuggle explosives into the cargo. The primary means of assuring safety of cargo for shipment today is the "known shipper" program that subjects such cargo to minimal screening, combined with closer inspection of cargo that comes from unknown sources. Critics charge that existing programs are insufficient against the demonstrated threat against passenger aircraft. Opponents counter that a cargo screening program would be expensive and impractical. To date, no rigorous and objective evaluations or analyses have been conducted that would allow lawmakers to determine what approach is appropriate.

Ports

Technology. Many of the needs in port and supply chain security can be traced back to the requirement for faster, cheaper, and more reliable screening methods. Current screening methods at U.S. ports are relatively slow, are limited in the threats they can detect (primarily nuclear and radiological), can be fooled with shielding and other concealment methods, and generate many false positives that must be resolved by hand. Despite these deficiencies, there are periodically calls for screening 100 percent of the cargo that arrives at U.S. ports.

Cost-Effectiveness. More generally, however, we have yet to conduct a rigorous and integrated assessment of the security of the supply chain system from point of origin to point of destination.

---

[12] It is still unclear how the explosives got on the planes, though it is clear that the bombs were triggered by two female suicide bombers from Chechnya. Traces of RDX, a common component of military explosives, were found at the crash scene.

As a result, there is very little evidence about how the different elements of security work together; how much security the measures actually provide; or what impact they have on the cost of moving goods (whether measured in dollars or time). For example, does C-TPAT, the program under which firms certify their security procedures, lead to improvements in security? Does C-TPAT work more or less effectively than CSI, the program that uses technology and advance screening to assess the risk of container shipments? The lack of knowledge about effectiveness raises risks that we will overinvest in some measures when the funding could be more fruitfully applied to other measures.

System Fragility. Finally, and worth emphasizing, we know little about the port and supply chain system's ability to be reconstituted after an incident or to maintain operations during disruptions. Simulations suggest that the system could be quite fragile in the face of an attack, and we have little experience to help us understand what it would take to reestablish the chain.[13] Contingency planning in this area is important, and policies that promote the system's ability to withstand, absorb, and recover from shocks should be given priority.

Land Borders

Many of the issues not yet addressed with ports also remain for land border crossings. This is not surprising, since land border crossings are also an important component of the supply chain. In particular, it seems prudent to focus on developing technologies that will facilitate fast, inexpensive, and reliable screening of cargo and people. The "smart border" procedures put in place with Canada and Mexico also bear close examination. It is assumed that NEXUS, FAST lanes, and other programs will keep commerce flowing (or enable a rapid restart) after a disruptive incident. Games, simulations, and other exercises can help identify issues that need to be resolved so that the policies will work as planned in the event of another attack.

Summary

Since 9/11, security at U.S. borders has significantly increased. Much of the policy implemented after 9/11 reflects the principles of ''pushing the border out'' to extend the reach of our security

---

[13] *Port Security War Game: Implications for U.S. Supply Chains*, (Mark Gerencser, Jim Weinberg, and Don Vincent, Booz Allen Hamilton, February 2003; online at http://www.boozallen.com/media/file/128648.pdf as of August 2, 2006). See also "Ports, Trade, and Terrorism: Balancing the Catastrophic and the Chronic" (Edward E. Leamer and Christopher Thornberg, in Jon D. Haveman and Howard J. Shatz, eds., *Protecting the Nation's Seaports: Balancing Security and Cost*, San Francisco, Calif.: Public Policy Institute of California, 2006, pp. 37–52).

and “profiling out” less threatening people and cargo in order to focus on targets that require more scrutiny. These principles have made border control more manageable, though they have by no means resolved certain broader issues of security.

Simultaneous with the programmatic initiatives that have increased border security is the sobering fact that we do not know very much about the effectiveness of individual border security programs, or about how various programs work together to affect commerce, costs, and security. As a consequence, we have very little idea about where to invest effectively in border security.

One reason we lack the template for investment in border security is that we also lack an integrated border control strategy. A national border control strategy is urgently needed to help establish priorities in both policy development and technology.

For these reasons, the establishment of a homeland security center of excellence on border security is strongly advisable. Border security is a dynamic, challenging problem that sustained, systematic and independent inquiry could productively address.