50. Homeland Security

Policymakers should

- make better screening of visitors at points of entry to the United States the top priority for the Department of Homeland Security and ensure that such screening is tied to terrorist databases;
- focus DHS's efforts on a few areas that will make a significant difference in preventing future terrorist attacks, rather than trying to do everything, and eliminate efforts that are only effective at the margins;
- make it clearer to the public that homeland security efforts cannot make the country absolutely safe against possible terrorist attacks;
- ensure the homeland security efforts are not disproportionately focused on defending against the last attack, for example, another September 11 or the Madrid train bombings, at the expense of other vulnerabilities that need to be remedied;
- not rush to reorganize the intelligence community as a way to fix perceived problems and to satisfy the public's need to feel safer; and
- ensure that civil liberties are not sacrificed for unneeded and ineffective homeland security measures.

A paramount responsibility of the federal government as set forth in the Constitution is to ''provide for the common defense.'' But in the largest open society in the world, providing homeland security is a daunting task. Some of the vulnerabilities include the 2,000-mile-long U.S.-Mexican border, the 3,900-mile-long U.S.-Canadian land border, and 2,300 miles of border over water between the United States and Canada; thousands of bridges, sports stadiums, and shopping malls; and hundreds of skyscrapers and nuclear power plants. Defending against the possibility of terrorist attacks with weapons of mass destruction may be even more challenging.

The Al Qaeda terrorist network poses a unique threat to the United States. Al Qaeda is the one and only terrorist group with demonstrated global reach and willingness to attack the U.S. homeland. Al Qaeda is an agile, nonbureaucratic adversary that has the great advantage of being on the offense—knowing when, where, and how it will attack. Al Qaeda operatives will take advantage of the poor coordination among military, intelligence, law enforcement, and other responsible bureaucracies to exploit gaps in defenses. No other security threat to the United States rivals this one. To fight this nontraditional threat, the U.S. government must think more innovatively and try to be as nimble as the opponent. Indeed, this is the difficult task laid at the doorstep of the Department of Homeland Security.

In taking on this task, it is important to recognize the hard truth: providing absolute and perfect defense against any and all future potential terrorist attacks is impossible. The nature of terrorism is to morph and adapt, to flow around obstacles, and to find the path of least resistance. The problem of trying to defend against terrorism is best illustrated in a statement by the Irish Republican Army after a failed attempt to kill British prime minister Margaret Thatcher in 1984: ''Remember, we only have to be lucky once. You will have to be lucky always.'' That is no less true for the U.S. government defending against Al Qaeda. Homeland security starts with knowing that a perfect defense against terrorism is not possible.

The problem of homeland security is so vast that the DHS will be tempted to do everything. The nature of bureaucracy is to grow and to do more. This is exactly what the department needs to avoid at all costs. To be effective, the department must do everything it can to be as nimble, responsive, and adaptive as our terrorist enemy.

Therefore, instead of trying to do the impossible or attempting to do everything and doing nothing well, homeland security must focus on those threats that pose the most catastrophic consequences and for which there are cost-effective defenses. First and foremost, that means not focusing on the last attack and disproportionately directing homeland security efforts against preventing the same thing from happening again. The March 2004 Madrid train bombings are proof enough that we should not be obsessed with hijacked airplanes. And even with airplanes, hijackings are not the only terrorist threat—passengers with explosives in carry-on baggage are a demonstrated threat to commercial airliners and the effect of such a terrorist attack could be even more chilling for the airline industry and the economy than were the attacks of September 11, 2001.

Preventing Terrorist Entry into the United States

The first priority for homeland security must be to prevent terrorists from entering the country. This is the single most important thing DHS can do to reduce the likelihood of another terrorist attack. It is important to remember that none of the 19 hijackers sneaked into the country the way hundreds of thousands of illegal immigrants come across the U.S.-Mexican border every year. Instead, they entered the United States via known points of legal entry, as millions of visitors to the United States do each year. Therefore, we need to put systems and procedures in place so that known or suspected terrorists can be stopped at the border by the appropriate authorities. The most crucial aspect is ensuring that information from the appropriate agencies (e.g., CIA, FBI, Interpol) about known or suspected terrorists is made directly available in real time to those people responsible for checking passports, visas, and other immigration information.

In theory, US-VISIT (Visa and Immigrant Status Indicator Technology) is supposed to screen for potential terrorists before they enter the country. In practice, however, it seems misdirected. When it was unveiled in January 2004, DHS secretary Tom Ridge claimed, ''While processing more than 20,000 travelers . . . US-VISIT has matched 21 hits on the FBI Criminal Watch List, including potential entrants with previous convictions for statutory rape, dangerous drugs, aggravated felonies, and several cases of visa fraud.'' Instead of flagging garden variety criminals, what's really needed is a ''Google search'' at the borders where a person's name and passport number can be cross-referenced with U.S. and foreign terrorist databases. And biometric data screening—such as facial recognition technology to compare people to photographs in those databases—might also be a useful technology to employ if tied to relevant databases.

Preventing WMD Entry into the United States

The prospect of terrorists using weapons of mass destruction—chemical, biological, or radiological/nuclear—is something that must be taken seriously. For the terrorists, there are opportunity costs associated with acquiring WMD, and the strategy of DHS should be to take all reasonable, prudent, and cost-effective measures to make those costs as high as possible.

More than 15,000 containers enter the United States via ship and twice that many via truck on a daily basis. DHS undersecretary for border and

transportation security Asa Hutchinson has stated that his goal is to inspect 100 percent of the ''at risk'' shipments into the United States. That is probably the most realistic and cost-effective approach to increasing the opportunity costs to terrorists' ability to smuggle WMD into the country. ''At risk'' could be defined as containers shipped from or transiting through countries where terrorists are known to operate, where ownership of the vessel is suspect, where the entire manifest cannot be adequately accounted for, or where there might be suspicious activity with regard to the crew. Clearly, in order to streamline the process and not impede the flow of commerce, there should be maximum use of technology to detect and prevent illegal or otherwise unauthorized radiological, chemical, or biological materials from entering the country.

But our homeland security efforts must not be dominated completely by WMD. Terrorists can also use low-tech means. For example, concerns have been raised about the vulnerability of commercial aircraft to shoulder-fired anti-aircraft missiles (i.e., MANPADS or man-portable air defense systems). Given that such aircraft do not currently have defensive countermeasures against such missiles and that it would be virtually impossible to secure the requisite areas around airports (a several-mile radius) to prevent their use, prudence dictates that these types of weapons should also be on the watch list.

Ships, trains, and trucks carrying hazardous materials could be potential bombs (just as hijacked airplanes are potential missiles). The foiled Jordanian terrorist attack in April 2004 demonstrated how trucks laden with chemicals and explosives could be potent homemade chemical bombs. Of course, not every ship, train, or truck is a threat, and the need for security must be balanced by the need to ensure the free flow of goods, which is vital to the health of the U.S. economy. For example, in 2003, 37,000 trucks crossed the border between the United States and Canada and the two-way trade in goods and services between the two countries was more than $441 billion.

Protecting Critical Facilities

There are literally thousands of potential targets for possible terrorist attack. Even with an unlimited budget, it would be impossible to protect all of them because there are too many targets to protect and myriad ways in which they can be attacked. But the government would be remiss to ignore protecting a subset of critical targets—such as nuclear facilities and chemical facilities—whose destruction could have catastrophic conse-

82978$CH50 12-08-04 09:10:46

quences. The key to providing such protection is understanding the nature of the catastrophic event that we are trying to prevent, how that event could be precipitated by terrorists, and what barriers can be erected to reduce the threat or minimize the damage. As with homeland security writ large, it will probably not be possible to defend against every potential attack. But reasonable and prudent measures need to be taken to make it as difficult as possible for attacks with catastrophic consequences.

For example, nuclear power plants would be lucrative targets, but it is not simply a matter of providing increased security. The first concern is to safeguard nuclear material so that it can't be stolen for building a radiological weapon. Second, the plant itself must be protected to prevent terrorists from creating a disaster along the lines of Chernobyl. Similarly, security for chemical and biological facilities must be designed to prevent terrorists from creating an accident such as the 1984 Union Carbide chemical pesticide plant accident in Bhopal, India, which killed more than 3,000 people.

Aviation Security

There has been a tremendous emphasis on airline and airport security since September 11. That is only natural. But two truths need to be recognized. First, security did not fail on September 11. The hijackers simply took advantage of a loophole in security, demonstrating that the terrorist mindset is to find the path of least resistance. Second, although we must guard against it, the likelihood of terrorists hijacking jetliners to be used as weapons of mass destruction is probably relatively low given all the new security measures and procedures.

Future terrorist tactics may not be to use jetliners as missiles, but simply to blow them up and kill as many people as possible. Since January 1, 2003, the Transportation Security Agency has screened 100 percent of checked baggage at all 429 commercial airports across the United States to check for explosive devices. But it's not just passengers and their checked baggage that are of concern. As demonstrated by the two Russian airliners blown up in August 2004, carry-on bags with explosives are a real threat. Air cargo (on both passenger and cargo-only aircraft) is currently not inspected 100 percent of the time. Greater emphasis needs to be placed on security for airport operations, especially for those people with access to aircraft (e.g., ground crews, baggage handlers, etc.). Airport perimeter security is also an issue that needs to be addressed.

Emergency Preparedness and Response

The post-9/11 reality that we have to be willing to accept is that, given enough time and opportunities, a determined terrorist group will likely eventually succeed in attacking the United States. Hopefully, it will not be another attack that results in the kind of mass casualties experienced on September 11. But despite all efforts to prevent further terrorist attacks, it is vitally important that the Department of Homeland Security is prepared to respond to such attacks.

Education

First and foremost, the public needs to be educated about how to be prepared for and respond to terrorist attacks, especially the potential use of chemical, biological, or nuclear/radiological weapons. Solid, science-based information needs to be made available about the effects of such weapons and what can be done to mitigate their effects. Resource directories must be published. People need to know where to go and whom to contact in the event of an emergency. And it is just as important that people know what not to do.

In short, if there are effective means of providing protection against certain types of possible terrorist attacks (e.g., potassium iodide used to protect the thyroid gland from the effects of exposure to the radioactive iodine from a dirty bomb), the Department of Homeland Security needs to let people know exactly what those are, how they work, how to use them, and where they can be obtained.

Prevention

It may be possible to take preventive measures against the effects of terrorist attacks, particularly against the prospect of biological pathogens. We have already seen and experienced the use of anthrax by some unknown person or group. We understand that the deadly smallpox virus—if introduced intentionally into a highly mobile population—could have widespread catastrophic effects. Rather than waiting and responding after the fact, it would be more prudent to take preventive measures beforehand.

The president's smallpox vaccination policy is a good example of such action. The best defense against smallpox is a vaccinated population—even just a partially vaccinated population. Unfortunately, that policy is being met with some resistance. There appears to be a reluctance on the part of the first-response force—the very people the rest of the population will depend on in the event of an attack—to be vaccinated. If we cannot

82978$CH50 12-08-04 09:10:46

even vaccinate our first responders, how can the population reasonably expect that the first responders will be able to vaccinate everyone else? And if the first responders are not getting vaccinated, what does that mean for a plan to allow people to make their own decision about receiving the vaccination?

Emergency Response

As was shown on September 11, emergency response to a terrorist attack (just as with a natural disaster) is at the local level. Therefore, instead of being spent in Washington, a large chunk of the money authorized and appropriated for homeland security by the Congress should be given to state and local governments to allow communities to assess their needs and how best to meet them. Some of that money would likely be spent on improving first responder capabilities, while some would be spent on improving communications and information-sharing capabilities (but not necessarily providing radios that first responders need for their day-to-day duties and responsibilities). But we must, above all, understand that emergency response cannot be accomplished with a federally mandated, top-down approach. The federal government should consider itself a coordinator that can provide guidance and information (and funding, when and where necessary) for emergency response. But the federal government cannot become the micromanager of emergency response, setting mandated guidelines and requirements for local communities with a cookie cutter approach. What is appropriate for a large and densely populated metropolitan area may be overkill (and financially unattainable) for a rural community.

Intelligence

The 9/11 Commission recommended sweeping changes to the U.S. intelligence community in response to failures related to the September 11 attacks. Although the commission was careful not to claim that the attacks could have been prevented, the public's perception seems to be that fixing problems related to intelligence—primarily communication and information sharing—will prevent another September 11. The public's desire to feel safe from another terrorist attack and the impulse to look to the federal government to provide that safety is certainly understandable, but that does not mean that the 9/11 Commission's recommendations are sacred and should be implemented without question.

Resolving the problem of communication and information sharing among the 15 different federal agencies with intelligence functions requires a careful assessment of the costs, benefits, and risks associated with reorganization vs. reform. It is not a question of either-or, but of achieving the right balance. Are there duplicative functions that can be eliminated or consolidated? Do U.S. intelligence-gathering and analysis requirements require 15 different agencies? The important thing is to cut before pasting rather than just pasting together a new government bureaucracy (as was done in creating the Department of Homeland Security). Does reorganization in and of itself break down the barriers to effective communication and information sharing? Or is making the cultural shift from a ''need to know'' to ''need to share'' paradigm more of a management and leadership issue?

Admittedly, having 15 different agencies that are not part of an integrated management structure is unwieldy and inefficient. But there are downside risks that must be considered before rushing to consolidate the intelligence community. It is important to remember that intelligence analysis is not an exact science. Competing points of view and the ability to dissent are an important and healthy part of the intelligence process. Consolidating the intelligence function (whether under the aegis of a cabinet-level secretary as recommended by the 9/11 Commission or the Bush administration's approach of a director who reports to the president) might actually decrease the freedom for intelligence analysts to disagree. The result could be more of the groupthink that seemed to plague the CIA's assessment of Iraq's WMD, instead of just a single agency affecting the broader intelligence community. So there are good reasons to keep intelligence separated rather than under the umbrella of a single person and unitary management control.

Before trying to reorganize the intelligence community, it would be useful to assess how well the Department of Homeland Security has been in getting what were the 23 disparate federal agencies that comprise the department to communicate and share information. The bottom line is that a headlong rush to fix what is perceived as broken in the intelligence community may not solve the real problems, may create other problems, and may give the public a false sense of security that it is safe from another September 11.

Civil Liberties

Finally, all homeland security actions must take into account civil liberties implications. We must heed Benjamin Franklin's admonition that

82978$CH50 12-08-04 09:10:46

''they that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.'' Before the government infringes on civil liberties, it must pass a litmus test: the government must demonstrate that any proposed new powers are essential, that they would be effective, and that there is no less invasive way to accomplish the same security goal.

Ultimately, we must remember that although terrorists may take advantage of our liberties to exploit vulnerabilities in our society, our liberties are not the problem in trying to defend against terrorism. In the final analysis, homeland security means securing the Constitution and Bill of Rights, not just the country itself.

Suggested Readings

de Rugy, Veronique, and Charles V. Peña. ''Responding to the Threat of Smallpox Bioterrorism: An Ounce of Prevention Is Best Approach.'' Cato Institute Policy Analysis no. 434, April 18, 2002.

Flynn, Stephen. *America the Vulnerable.* New York: HarperCollins, 2004.

Harris, James W. ''Building Leverage in the Long War: Ensuring Intelligence Community Creativity in the Fight against Terrorism.'' Cato Institute Policy Analysis no. 439, May 16, 2002.

Lynch, Timothy. ''Breaking the Vicious Cycle: Preserving Our Liberties While Fighting Terrorism.'' Cato Institute Policy Analysis no. 443, June 26, 2002.

Taylor, Eric R. ''Are We Prepared for Terrorism Using Weapons of Mass Destruction? Government's Half Measures.'' Cato Institute Policy Analysis no. 387, November 27, 2000.

_____. ''The New Homeland Security Apparatus: Impeding the Fight against Agile Terrorists.'' Cato Institute Foreign Policy Briefing no. 70, June 26, 2002.

—Prepared by Charles V. Peña

82978$CH50 12-08-04 09:10:46