

A Broad Take on America's Current Homeland Security

Testimony of Michael O'Hanlon, Brookings Institution, March 8, 2007, before the House Committee on Homeland Security's Subcommittee on Border, Maritime and Global Counterterrorism¹

A critical issue in any national security agenda for the United States is how to protect America against the most immediate and direct threat to U.S. security—the possibility that future attacks like those of September 11, 2001 will again kill large numbers of American citizens here in the homeland. If they able to obtain weapons of mass destruction, particularly nuclear weapons or advanced biological agents, the toll could easily be 10 or even 100 times worse. Politically, the issue of counterterrorism and homeland security is of manifest importance too. The Bush administration achieved a greater advantage over Democrats in general and Senator John Kerry in particular on this issue than on any other in the 2004 presidential race.

Homeland security is a matter on which this Congress as well as the next Congress and administration will have to make great progress because much remains to be done. That said, the arguments of critics are often too harsh and sweeping. Much remains to be accomplished, to be sure, in protecting the United States against al Qaeda and related groups. And on some questions, such as the long-term battle of ideas and the execution of the Iraq war, the Bush Administration's record should indeed be subject to severe criticism. But it is misleading to suggest that the Bush administration has been

¹ Much of this comes from Kurt Campbell and Michael O'Hanlon, *Hard Power: The New Politics of National Security* (Basic, 2006); and Michael d'Arcy, Michael O'Hanlon, Peter Orszag, Jeremy Shapiro, and James Steinberg, *Protecting the Homeland 2006/2007* (Brookings, 2006).

weak on what might be termed the hard power aspects of the homeland security agenda—improving the country’s defenses against their aspirations for further attacks. Democrats and moderate Republicans who would challenge the Bush legacy and chart a future path for the country of their own need to develop a clearer sense of what has been achieved, and of what must still be done. More important than the politics of it, of course, America’s security and the well-being of its citizens depend on such a clear-headed assessment and sound policy agenda from their future political leaders.

The war on terror has been a hot subject in American politics at least since President Bush broadened the scope of his definition of the effort to include the doctrine of military preemption and the overthrow of the Saddam Hussein regime. In fact, it has been controversial even longer. Mr. Bush’s State of the Union speech of January 29, 2002—also known as the “axis of evil” speech—signaled a broader scope for the war on terror than originally described by the president in his address to another joint session of Congress the previous September 20, just nine days after the September 11 attacks.² The debate over the creation of a new Department of Homeland Security was central in the Congressional midterm elections of 2002, in which President Bush campaigned more actively than presidents typically do at such points in the political cycle. Mr. Bush had originally opposed the idea of a new department, which in fact was initially Senator Joseph Lieberman’s idea. But after accepting the notion in the spring of 2002, and proposing a bill to create it that year, the president argued that Democrats were placing

² See President George W. Bush, “Address to a Joint Session of Congress and the American People,” September 20, 2001, available at www.whitehouse.gov/news/releases/2001/09/print/20010920-8.html; President George W. Bush, “State of the Union Address,” January 29, 2002, available at www.whitehouse.gov/news/releases/2002/01/print/20020129-11.html; and President George W. Bush, “National Security Strategy of the United States of America,” September 17, 2002, available at www.whitehouse.gov/nsc/nssall.html.

their political interests in defending unions ahead of their obligations to help defend the American people. Democrats countered that protecting workers remains a critically important goal for the country itself, and that a federal workforce deprived of core rights and protections might suffer weaker morale and as a result perform suboptimally in trying to protect the country. But Mr. Bush's argument seemed to resonate with voters, helping Republican candidates win several tight races and take back the Senate.

Democrats have responded by arguing that the Bush Administration has tolerated glaring gaps in the nation's protection against terrorism here at home even as it has prosecuted wars abroad with vigor. For example, they point to the very slow integration of terrorist watchlists during Mr. Bush's first term, and to the administration's weak efforts to help states and localities improve their counterterror capabilities.

The president has weathered sharp critiques in part because his critics have been less than skilful. That said, Democrats have arguably often raised the wrong issues or done so in the wrong way—on both policy and political grounds. In the 2004 presidential race, for example, Senator Kerry and President Bush competed to see which could more quickly and convincingly align himself with the recommendations of the 9/11 commission on matters such as reform and restructuring of America's intelligence community, with Kerry often criticizing Bush for delay. But many of the key changes to intelligence that were most needed to break down stovepipes in the system had already been fixed prior to the release of that report. Critics of the Bush Administration from both parties have also argued that the Patriot Act did not give proper due to the civil liberties of American citizens—just as detention policies at Guantanamo Bay and prison policies at Abu Ghraib have hurt America's reputation for fairness and created even more

hatred of this country that has helped al Qaeda with its recruiting worldwide. These criticisms of the latter policies have generally been appropriate and fair. But the Patriot Act, which updated surveillance methods for the era of computers and cell phones, broke down barriers to sharing of intelligence across agencies, and strengthened standards on documents such as passports was far better legislation than critics often allowed. By so strongly condemning it, many Democrats therefore set themselves up for Bush Administration counterattack.

Finally, Democrats and other administration critics have often purported that the Bush Administration did not do enough to train and equip first responders around the country to deal with possible attacks. In some ways that charge is correct, but it would have been expensive folly to invest tens of billions of dollars in protective gear and rudimentary training for all the nation's first responders, as often proposed. A more targeted set of investments—focused on the most likely terror targets in the country geographically, as well as on the types of technologies and training that provide the most capability per dollar—makes a good deal more sense.³

I argue here for several specific policy initiatives on homeland security, and somewhat greater spending by the federal government as well as the private sector, but not for a kitchen-sink approach to the problem or any radical increase in resources. In dealing with this huge set of challenges, clear priorities and a clear conceptual framework for guiding investments are essential. Otherwise costs can be exorbitant, and less-important tasks may distract attention from more important ones.

³ For more on some of these issues, see Richard A. Falkenrath, "The 9/11 Commission Report: A Review Essay," *International Security*, vol. 29, no. 3 (Winter 2004/05), p. 184.

Specifically, I advocate new initiatives to encourage the private sector to protect itself more effectively, especially in sectors such as the chemical industry and high-rise buildings; to develop a more comprehensive system for cargo security on airplanes and in shipping containers entering the country and in trucks and trains carrying toxic materials domestically; to create national standards for driver's licenses with biometric indicators (not photos) and, similarly, improvement of the biometric indicators used on US passports; to encourage more large-city police departments to build dedicated counterterror cells as New York has done; and to develop a quick-manufacture capacity for vaccines and antidotes to new pathogens that it does not now possess.

Before developing the logic behind these prescriptions, however, it is first important to assess where we stand in the war on terror. (Those not wishing this background can certainly feel free to skip ahead a section.)

A Status Report for the War on Terror

In developing their policies and positions on counterterrorism strategy for the coming years, candidates need to begin with a clear sense of the facts. While much is still undone, the fact is that much has also been accomplished in the last five years. Much of that increase in safety has come from offensive operations abroad—the military overthrow of the Taliban and associated attacks against al Qa'eda, as well as the intelligence and covert operations conducted by the United States in conjunction with key allies such as Pakistan and Saudi Arabia.

Homeland security spending is up by at least 300 percent—hardly fitting the charge that its funding is on “life support” that some critics have offered. U.S.

intelligence spending is now reportedly up to \$44 billion a year, as much as \$10 billion more than estimated levels from the 1990s, with nearly 100,000 individuals working for American intelligence agencies.⁴ There is more debate in the analytic process, and a clearer emphasis in finished reports on the uncertainties of various types of assessments (to avoid the mistakes not only of 9/11, but of the Iraqi WMD experience).⁵ Terror watch lists are now integrated, perhaps belatedly; domestic and foreign intelligence operations no longer have strong “firewalls” between them, and that change was made quickly.

The Patriot Act, whatever its problems in insufficiently protecting civil liberties, or its possible over-exuberance in allowing subpoenas of library records and the like, on balance has been good legislation. Democrats and other Bush administration critics need to acknowledge that updating wiretap authority for the era of the internet, allowing “roving wiretaps” not fixed to one phone or location, breaking down barriers between the FBI and CIA, making banks report suspicious money transfers, requiring visa-waiver countries to have biometric indicators on their passports, prohibiting possession of dangerous biological materials without good research or medicinal reasons, and similar measures were overdue and prudent.⁶ There is room for debate about specific provisions of the Patriot Act, but it is neither sound policy nor sound politics to rail against it categorically as critics have sometimes done.

Similarly, in the debate over domestic eavesdropping, Democrats and many Republicans have been right to expect Mr. Bush not to disobey the law (or push it all the

⁴ Mark Mazzetti, “Spymaster Tells Secret of Size of Spy Force,” *New York Times*, April 21, 2006.

⁵ John A. Kringen, “How We’ve Improved Intelligence,” *Washington Post*, April 3, 2006, p. 19.

⁶ Charles Doyle, “The USA Patriot Act: A Sketch,” *CRS Report for Congress* (Washington, D.C.: Congressional Research Service, April 18, 2002).

way to the breaking point). Asserting greater executive privilege should not extend to flouting existing legislation or claiming to find incredulous loopholes within it. But Democrats should also recognize that obtaining warrants in advance for all eavesdropping, even from a court set up to do so quickly and secretly, is neither practical nor prudent, as argued convincingly by law professors and judges with experience in the field such as Philip Bobbitt and Richard Posner.⁷

On Guantanamo, critics have again been largely right to criticize as un-American and counterproductive the willingness of the administration to hold detainees indefinitely without charges or any type of due process. This has been a huge policy mistake of the United States. It reflects some partially correct observations—that terrorists are not like soldiers, that introducing the cases of detainees into normal American criminal courts is not practical given the kinds of classified information, including sources and methods on how we monitor possible terrorists, that would then have to be discussed openly. On the whole, however, the Bush administration’s treatment of terrorist detainees has caused far more damage to the United States than any of the policy’s authors seem to appreciate—and far more damage than can be easily or quickly repaired.

Yet critics must themselves be careful. Tone matters when critiquing such policies, for Bush administration critics will not succeed when they sound as if they fear a hypothetical executive threat to civil liberties more than they fear another al Qaeda attack. So does any suggestion that the country is now safe enough that we can always place every last hypothetical civil liberties concern ahead of confronting al Qaeda. In this regard, a recent quote by a senior Democratic political strategist, reflective of a good deal

⁷ Richard A. Posner, “A New Surveillance Act,” *Wall Street Journal*, February 15, 2006, p. 16; and Philip Bobbitt, “Why We Listen,” *New York Times*, January 30, 2006, p. A27.

of ongoing thinking, is in our view wrongheaded. In regard to the eavesdropping issue, he stated early in 2006 that “I don’t think the national security attack works this time...we have a politically weakened president whose poll numbers are down and whose credibility is under increased scrutiny.”⁸ This is exactly the wrong kind of political thinking to engage in for anyone wishing to win an election.

Guantanamo has been a travesty. A smarter policy would recognize the need for special legal procedures for suspected terrorists but create a legal firewall inside the government between those charged with arresting and holding terrorists, on the one hand, and those determining their fate on the other. In particular, the administration should have moved far more quickly to create an independent authority inside the executive branch with the binding power to release detainees it deemed no longer a threat, and it should have set up a regularized hearing process to assess the status of detainees promptly and fairly. But it is also perfectly clear that trying terrorist cases in normal criminal courts would have been unworkable.

The United States now processes and shares information about specific individuals suspected of ties to terrorism much more efficiently throughout the federal government. It does so through increased integration of databases (even if that process took longer than it should have after 9/11), and greater collaboration between the FBI and the intelligence community (which began to occur shortly after 9/11). These initial efforts have now been reinforced by the passage of the Intelligence Reform and Terrorism Prevention Act of 2004 that restructured the intelligence community and created the

⁸ Jim VandeHei, “Rift Between Parties Over NSA Wiretapping Grows,” *Washington Post*, January 26, 2006, p. 4.

position of director of national intelligence. These linked databases enable more effective offensive operations abroad and homeland security operations within American borders.

The share of FBI resources devoted to counterterrorism has doubled, and the combined CIA/FBI personnel working on terrorist financing alone have increased from less than a dozen to more than 300 since September, 2001.⁹ International cooperation in sharing information on suspected terrorists has improved. Many close allies, such as France and Britain, have been helpful for many years, but intelligence sharing on known al Qaeda threats has also become reasonably good with states such as Pakistan and Saudi Arabia—in part because some such states now take the jihadist threat to their own interests more seriously than they used to.

Air travel is also much safer today than before 9/11. The United States now conducts screening of all passenger luggage, requires hardened cockpit doors on all large American commercial aircraft, deploys thousands of air marshals on commercial carriers, and allows armed pilots on commercial and cargo flights.

Suspicious ships entering U.S. waters are now screened more frequently, and containers coming into the United States are two to three times more likely to be inspected than before. Hundreds of millions of doses of antibiotics and enough smallpox vaccine for every man, woman, and child in the United States have been stockpiled.¹⁰ Oversight rules have been tightened on labs working with biological materials (including

⁹ Vicky O'Hara, "Terrorist Funding," National Public Radio, Morning Edition, November 20, 2003; Speech of George W. Bush at the FBI Academy, Quantico, VA, September 10, 2003; and Philip Shenon, "U.S. Reaches Deal to Limit Transfers of Portable Missiles," *New York Times*, October 21, 2003, p. A1.

¹⁰ Tom Ridge, "Since That Day," *Washington Post*, September 11, 2003, p. 23.

background checks on lab employees).¹¹ Terrorism insurance is backstopped by a new federal program, recently renewed in 2005.

Well-known bridges and tunnels are protected by police and National Guard forces during terrorism alerts. Nuclear reactor sites have better perimeter protection than before.¹² Federal agencies are required to have security programs for their information technology networks. Many private firms have backed up their headquarters and their databanks so that operations and information systems could survive the catastrophic loss of a main site.¹³

What all of these efforts amount to, in short, is this: we have prepared fairly well to fight the last war—that is, to stop the kinds of attacks that the United States has already experienced. Importantly, the United States has also gotten much better at trying to prevent attacks by tracking suspected terrorists more assertively. Since prevention should be seen as the most crucial stage of the homeland security effort, more important for example than hardening most individual targets, this is real progress.

The United States cannot be complacent, however. We have done much less than we should in the way of detailed preparation to thwart other kinds of plausible strikes. It made sense to move quickly to prevent al Qaeda, with its longstanding interest in airplanes, from easily repeating the 9/11 attacks. But it is high time to do a more comprehensive and forward-looking job of protecting the American people.

¹¹ Martin Enserink, "Facing a Security Deadline, Labs Get a 'Provisional' Pass," *Science*, November 7, 2003, p. 962.

¹² There may be some gaps in these types of protective measures to date, but the overall level of security is generally good. See Statement of Jim Wells, General Accounting Office, "Nuclear Regulatory Commission: Preliminary Observations on Efforts to Improve Security at Nuclear Power Plants," GAO-04-1064T, September 14, 2004.

¹³ John Moteff, "Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives," Congressional Research Service Report for Congress RL32357, April 16, 2004, p. 2.

Al Qaeda may not be as capable as before of "spectacular" attacks in coming years. It is, however, certainly still capable of using explosives and small arms, with considerable lethality.¹⁴ There have not been more attacks within the United States. But according to an October, 2005 speech by President Bush, the United States has disrupted three attempted al Qaeda strikes inside the United States, and intercepted at least five plots to case targets or infiltrate terrorists into this country.¹⁵ There were serious worries that al Qaeda would use truck bombs to destroy key financial institutions in New York, Newark, and Washington in 2004.¹⁶ The "shoe bomber," Richard Reid, attempted to destroy an airplane headed to the United States in 2002.¹⁷ U.S. intelligence reports in early 2005 suggested the possibility of attacks using private aircraft or helicopters.¹⁸ Al Qaeda prisoner interviewers and confiscated documents suggest other possible attacks ranging from blowing up gas stations to poisoning water supplies to using crop dusters to spread biological weapons to detonating radioactive dirty bombs.¹⁹

The years 2002, 2003, and 2004 were among the most lethal in the history of global terrorism, with attacks afflicting a wide swath of countries from Spain to Morocco to Tunisia to Saudi Arabia to Pakistan to Indonesia—and of course Iraq.²⁰ The pattern

¹⁴ David Johnston and Andrew C. Revkin, "Officials Say Their Focus Is on Car and Truck Bombs," *New York Times*, August 2, 2004, p. A13.

¹⁵ President George W. Bush, Speech on Terrorism at the National Endowment for Democracy, October 6, 2005, available at www.whitehouse.gov [accessed October 6, 2005].

¹⁶ Eric Lichtblau, "Finance Centers Are Said to Be the Targets," *New York Times*, August 2, 2004, p. 1.

¹⁷ Shaun Waterman, "Al Qaeda Warns of Threat to Water Supply," *Washington Times*, May 29, 2003, p. 6; and Eric Lichtblau, "U.S. Cites al Qaeda in Plan to Destroy Brooklyn Bridge," *New York Times*, June 20, 2003, p. 1.

¹⁸ Eric Lichtblau, "Government Report on U.S. Aviation Warns of Security Holes," *New York Times*, March 14, 2005, p. A1.

¹⁹ Matthew Brzezinski, *Fortress America* (New York: Bantam Books, 2004), pp. 16-17.

²⁰ See Gilmore Commission (Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction), Fifth Annual Report, *Forging America's New Normalcy: Securing Our Homeland, Preserving Our Liberty* (Arlington, Va.: RAND Corporation, December 15, 2003), p. 1; Alan B. Krueger and David D. Laitin, "'Misunderestimating' Terrorism,"

continued in 2005, a year during which the number of global terrorist attacks again grew relative to the year before (though new counting methods and limits upon the public release of data make it somewhat difficult to compare precisely from year to year).²¹ The July 7 London attacks that year should have vividly reminded westerners in general of their continued vulnerability.²² According to Hillary Peck of the RAND Corporation, even though fewer Americans were the victims, global fatalities from terrorist action exceeded the 2001 total of 4,555 in both 2004 and 2005 (the death toll exceeded 5,000 in each of those latter two years).²³

Al Qaeda has clearly been weakened at the top since 9/11. That said, it remains extremely dangerous, and not just because bin Laden and al-Zawahiri remain at large.²⁴ Al Qaeda is now less of a vertical organization than an ideology or a method used by collection of loosely affiliated local groups that share similar goals. They also watch and learn from each other, through television and the internet and extended family connections and other social networks.²⁵ Former CIA Director Tenet put it succinctly in 2004: "Successive blows to al Qaeda's central leadership have transformed the

Foreign Affairs, vol. 83, no. 5 (September/October 2004), p. 9; and Susan B. Glasser, "U.S. Figures Show Sharp Global Rise in Terrorism," *Washington Post*, April 27, 2005, p. 1.

²¹ Warren P. Strobel, "U.S.: Terrorist Attacks Increased Last Year," *Philadelphia Inquirer*, April 21, 2006.

²² Richard Benedetto, "Americans Expect Attacks, Poll Finds," *USA Today*, July 12, 2005, p. 1.

²³ Will Marshall and Jeremy Rosner, "Introduction: A Progressive Answer to Jihadist Terror," in Will Marshall, ed., *With All Our Might: A Progressive Strategy for Defeating Jihadism and Defending Liberty* (Lanham, Maryland: Rowman & Littlefield Publishers, Inc., 2006), p. 2.

²⁴ See Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004).

²⁵ The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission), *Implementing the National Strategy* (December 2002), p. 11; and Douglas Farah and Peter Finn, "Terrorism, Inc.," *Washington Post*, November 21, 2003, p. 33. On the assertion that modern terrorist groups watch and learn from each other, see Bruce Hoffman, "Terrorism Trends and Prospects," in Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, and Michele Zanini, *Countering the New Terrorism* (Santa Monica, Calif.: RAND, 1999), pp. 8-28; and on the nature of al Qaeda and affiliated as well as sympathetic organizations, see Paul R. Pillar, *Terrorism and U.S. Foreign Policy* (Washington, D.C.: Brookings, 2001), pp. 54-55.

organization into a loose collection of regional networks that operate more autonomously."²⁶

There are benefits from dispersing al Qa'eda in this way; the near-term risk of sophisticated catastrophic attacks has probably declined as a result. But the risk of smaller and sometimes quite deadly strikes clearly has not—and the possibility of further catastrophic attacks may well increase again in the future. To underscore the enduring risks, a U.N. study in early 2005 argued that al Qa'eda continues to have easy access to financial resources and bomb-making materials.²⁷

Great benefits were gained by depriving al Qa'eda of its sanctuary in Afghanistan in Operating Enduring Freedom. Al Qa'eda may learn to reconstitute itself with a less formal and more virtual and horizontal network, however. It could also avoid terrorist watch lists with some effectiveness, for example by using new recruits – including possibly women, non-Arabs, and European passport holders—to conduct future attacks against Western countries.²⁸ The United States is fortunate not to have, as far as we know, many al Qa'eda cells presently on its soil, as several European countries do. It is not a foregone conclusion that things will stay this way, however.²⁹ For all these reasons, it is hard to disagree with former CIA Director Porter Goss, who told Congress in February 2005 that "It may be only a matter of time before al Qa'eda or another group attempts to use chemical, biological, radiological, and nuclear weapons."³⁰

²⁶ Cited in Daniel L. Byman, "Homeland Security: We're Safer Than You Think," *Slate*, August 2, 2004.

²⁷ Leyla Linton, "Al-Qa'eda, Taliban Can Still Launch Attacks, Report Says," *Philadelphia Inquirer*, February 16, 2005.

²⁸ "Washington in Brief," *Washington Post*, July 17, 2004, p. A5.

²⁹ Byman, "Homeland Security," *Slate*, August 2, 2004; and ABC News, "No 'True' Al Qa'eda Sleeper Agents Have Been Found in U.S.," *abcnews.com*, March 9, 2005.

³⁰ Bill Gertz, "Goss Fears WMD Attack in U.S. 'A Matter of Time,'" *Washington Times*, February 17, 2005, p. 3.

The Iraq war, whatever its other merits, has probably not alleviated the global terrorism problem. Indeed, it may have worsened it, by aiding al Qaeda's recruiting efforts and providing jihadists a focal point to practice their crafts and establish new networks. To quote Goss again, "Islamic extremists are exploiting the Iraqi conflict to recruit new anti-U.S. jihadists. These jihadists who survive will leave Iraq experienced and focused on acts of urban terrorism."³¹ The National Intelligence Council reached a similar conclusion in its 2004 report, *Mapping the Global Future*.³²

The Agenda for this Congress and the Next

Of course, it is not possible to defend a large, open, advanced society from all possible types of terrorism. The United States contains more than half a million bridges, nearly 500 skyscrapers, nearly 200,000 miles of natural gas pipelines, more than 2,800 power plants – the list of critical infrastructure alone is far too long to protect everything, to say nothing of subways, restaurants and movie theaters and schools and malls.³³ Certain special measures, such as providing extremely tight security around the nation's 104 nuclear power plants, clearly cannot be extended to all possible targets.³⁴

But by focusing on the worst possible attacks, the United States can establish priorities and make further progress in protecting the country. Several guidelines should inform future efforts, and politicians' efforts to speak to the American people about what broad principles should guide next steps in enhancing homeland security:

³¹ Dana Priest and Josh White, "War Helps Recruit Terrorists, Hill Told," *Washington Post*, February 17, 2005, p. 1.

³² National Intelligence Council, *Mapping the Global Future* (December 2004), p. 94.

³³ Richard K. Betts, "The Soft Underbelly of American Primacy: Tactical Advantages of Terror," *Political Science Quarterly*, vol. 117, no. 1 (Spring 2002), p. 30.

³⁴ On jamming, see "U.S. Homeland Defense Strategists," *Aviation Week and Space Technology*, September 6, 2004, p. 20.

First, while it was correct to focus initially on preventing al Qaeda from carrying out attacks similar to those of 9/11, we have prepared a bit too exclusively to fight “the last war.” Heeding the counsel of the 9/11 commission, we now need to stretch our imaginations a bit to identify other key national vulnerabilities, such as possible attacks on chemical plants or skyscrapers or the air circulation systems of stadiums

Second, we should focus first and foremost on prevention—that is, on obtaining good intelligence on terrorists, and impeding their movements and their financial transactions and their communications, rather than focusing on point defense of the nation’s key assets or on mitigating the consequences of successful attacks (the latter tasks are important but are not as optimal as preventive efforts).

Third, since we cannot protect everything, we should worry most about possible terrorist strikes that would cause large numbers of casualties. Only slightly less critically, we should focus intensively on preventing attacks that might cause only a relatively few casualties, but huge economic ripple effects, such as episodes of attempted smuggling that revealed gaping holes in shipping container security.

Here is another example of the latter type of scenario. If a shoulder-launched surface-to-air missile took down an airplane, casualties might be relatively modest—dozens or hundreds—a tragedy for those involved to be sure, but in and of itself not debilitating to the nation. The effects on the nation's air travel could be devastating, however. They also could endure much longer than those of September 11, 2001, since it would take a good deal of time to figure out a workable response to avoid future SAM attacks. Another example could be the use of a radiological weapon, which uses conventional explosive to disperse radioactive material, in an urban area. It would not

kill many people, but would likely cause mass panic. It would also probably require a very costly and time-consuming cleanup—as well as implementation of disruptive security measures throughout the country.³⁵

There are also general areas of homeland security where important progress has occurred in some ways but where key shortcomings remain. Consider America's vulnerability to biological attack. Although antibiotic stocks for addressing any anthrax attack are now fairly robust, means of quickly delivering the antibiotics are not.³⁶ Longer-term worries about biological attacks remain acute, since there could be many types of infectious agents for which antidotes and vaccines prove unavailable (or non-existent) when they are most needed.

As for air travel, most passengers are still not screened for explosives, cargo carried on commercial jets is usually not inspected either, and private planes face minimal security scrutiny. For all the security improvements that have been made for U.S. carriers, moreover, fewer have been made to many foreign carriers that transport large numbers of Americans to and from the United States.

More generally, the U.S. private sector has done very little to protect itself.³⁷ From chemical plants to trucking carrying hazardous shipping to skyscrapers, vulnerabilities are often acute and not far different from how they presented themselves prior to 2001.³⁸ Owners of private infrastructure know that the chances of any one facility they own being attacked are miniscule, so they are not apt to incur added costs—

³⁵ Peter D. Zimmerman with Cheryl Loeb, "Dirty Bombs: The Threat Revisited," *Defense Horizons*, no. 38 (January 2004).

³⁶ Lawrence M. Wein and Edward H. Kaplan, "Unready for Anthrax," *Washington Post*, July 28, 2003, p. A21.

³⁷ Statement of Richard Falkenrath before the Senate Committee on Homeland Security and Governmental Affairs, January 26, 2005, pp. 14-15.

³⁸ Statement of Richard Falkenrath before the Senate Committee on Homeland Security and Governmental Affairs, January 26, 2005, pp. 12-14.

and concede to shareholders and neighbors that their facilities might vulnerable—on their own volition. Yet viewed from a national perspective, these means that certain systemic vulnerabilities remain unaddressed.

The creation of the Department of Homeland Security has not automatically led to better protection against such threats, as the hapless response to Hurricane Katrina revealed. DHS has many capable and dedicated individuals serving within it. However, reorganizations can distract attention from efforts to identify remaining key American vulnerabilities and then mitigate them.³⁹ Carrying out a major governmental overhaul during what is essentially a time of war is a risky proposition. It is also not the way the country has typically responded to national crises. The Department of Defense was not created during World War II, but afterwards. The Goldwater-Nichols Pentagon reorganization in 1986 was carried out during a time of relative international peace.

Congress has improved its ability to address homeland security issues by creating dedicated authorization committees and appropriations subcommittees in both houses somewhat. Yet it has not gone far enough. These dedicated committees and subcommittees must share jurisdiction with many other committees and subcommittees that insist on a share of the decision-making power.⁴⁰ This approach breeds parochialism among the individual committees and subcommittees about the particular dimensions of homeland security they address. It can also reinforce the tendency for Congressmen to allocate precious homeland security dollars to their districts rather than to where they

³⁹ Statement of Richard Falkenrath before the Senate Committee on Homeland Security and Governmental Affairs, January 26, 2005, pp. 2, 7.

⁴⁰ For a similar critique of Congress's role, see 9/11 Commission, *The 9/11 Commission Report* (New York: W.W. Norton and Co., 2004), pp. 420-422.

might do the most good.⁴¹ Congress should ensure that homeland security committees and subcommittees should generally have exclusive jurisdiction over funding that is found within the homeland security realm.

In sum, then, much has been done in homeland security, and much remains to be done. That message, with that balanced tone, may be less appealing to politicians seeking to excoriate the Bush administration's record, but it is a fairer reflection of reality. In tone and temperament, it also conveys a seriousness of purpose Americans may appreciate more than the wanton partisanship of recent years. A candidate offering specific critiques not only can come across as more affable, but sends a message that he or she is seeking concrete, specific improvements in policy rather than opportunities for partisan attack that are of little use once in office.

The organizing philosophy of our future efforts on homeland security should be to protect against attacks with potentially catastrophic impact on the country, in human or economic or political terms. In the interest of cost effectiveness, where possible action should focus on prevention of attacks rather than site defense of potential targets or consequence mitigation after attacks have occurred. But a blend of all approaches will be needed:

- creating incentives for the private sector to protect itself more effectively, especially in sectors such as the chemical industry and high-rise buildings
- developing a better and much more rigorous security system for container cargo
- greatly expanding screening of cargo on airplanes

⁴¹ See Statement of Richard Falkenrath before the Senate Committee on Homeland Security and Governmental Affairs, January 26, 2005, p. 4.

- creation of national standards for driver’s licenses with biometric indicators (not photos) and, similarly, improvement of the biometric indicators used on US passports
- encouragement to more large-city police departments to build dedicated counterterror cells as New York has done
- with terror watch lists now largely integrated, movement to the next step in using information technology in the war on terror—creation of a “google-like” search capacity across different police and intelligence databases for correlations of suspicious behavior
- examination of how the country can develop a quick-manufacture capacity for vaccines and antidotes to new pathogens that it does not now possess. This could also be of great importance in addressing such scenarios as a possible mutation of the bird flu H5N1 virus to a form highly dangerous to humans.⁴²

It is always sound to begin discussion of a new homeland security agenda by focusing on intelligence—the front lines in the effort, and the most important type of homeland security effort since an ounce of prevention is worth a pound of cure (or consequence management). Since there is too much to protect in this country, the only way to make homeland security successful is to stop most terrorists before they can even get in position to attempt an attack.

One key area of needed improvement in this domain is coordination between the federal government on the one hand and state and local governments on the other. Today, although the FBI runs the Joint Terrorism Task Forces (JTTFs) in major cities, and is beginning to help state and local police forces more effectively, it is very small

⁴² Kendall Hoyt, “Bird Flu Won’t Wait,” *New York Times*, March 3, 2006.

compared with police forces. That means it can have nothing like the same presence on the ground. In addition, while changes have occurred, it has been slow to change its traditional focus on solving criminal cases. An approach recommended recently by a team of Brookings scholars would use federal funds to expand local police intelligence and counterterrorism units in America's larger cities.⁴³ Today, only New York really takes this task seriously. The use of federal funds to recruit an extra 10,000 police officers for this purpose would cost around \$1 billion a year.

Other steps are needed too. Notably, despite the opposition of a number of states, federal standards for driving licenses must be mandated. U.S. security agencies should also create "data czars"-- to protect information, and also to facilitate its timely exchange when appropriate.

As Brookings scholar Jeremy Shapiro and Dean of the LBJ School of Public Policy James Steinberg have recently argued, the transatlantic homeland security agenda requires further work as well. For example, an assistance and extradition treaty was signed between the U.S. and E.U. in June 2003. But there is still a need for measures on both sides of the Atlantic that allow the admission of intelligence information as evidence in court while protecting against its disclosure.⁴⁴

There are also some areas where existing European efforts at homeland security exceed those of the United States. In particular, as Michael d'Arcy of King's College in London has argued, the U.S. choice of using just a facial image as the biometric indicator

⁴³ Michael d'Arcy, Michael O'Hanlon, Peter Orszag, Jeremy Shapiro, and James Steinberg, *Protecting the Homeland 2006/2007* (Washington, D.C.: Brookings, 2006), pp. 122-124.

⁴⁴ James Steinberg, "Intelligence Reform," in Michael d'Arcy, Michael O'Hanlon, Peter Orszag, Jeremy Shapiro, and James Steinberg, *Protecting the Homeland 2006/2007* (Washington, D.C.: Brookings Institution, 2006), pp. 27-30; and Jeremy Shapiro, "International Cooperation on Homeland Security," in d'Arcy, O'Hanlon, Orszag, Shapiro, and Steinberg, *Protecting the Homeland 2006/2007*, pp. 58-69.

in its passports is unwise. Photographs are inherently unreliable. The U.S. should follow the E.U. in incorporating fingerprints data, and ideally both sides of the Atlantic will move to using iris data in time.⁴⁵

Foreign airliners should also be expected to meet tighter security standards within short order. This problem is of particular concern outside the European Union. Deployments of hardened aircraft doors and air marshals are imperative. They are also overdue.

Considerable progress has been made in the US-VISIT program, which requires most people entering the United States to submit fingerprints and a digital photograph. These biometrics can then be checked against the DHS IDENT database and the records of visa holders. The United States should also speed up efforts to track the exits of visa holders. This is important to prevent people who have managed to get into the country on visa to overstay their legally allowed stay, with the possibility of conducting terror attacks over a long period of time.

There are also still major problems at the U.S. borders, which remain porous despite major improvements. The PATRIOT Act increased the number of patrol agents at the U.S.-Canadian border to 1,000, but more are needed, as evidenced by the continued high flow of people across the border. The SBI appears to be an initiative that in scale and scope is commensurate with the seriousness of this challenge. In this context, the United States and its neighbors should continue to move to a regime in which all people who cross the border, including passengers in cars, are individually screened. This is not standard practice today.

⁴⁵ Michael d'Arcy, "Technology Development and Transportation Security," in d'Arcy, O'Hanlon, Orszag, Shapiro, and Steinberg, *Protecting the Homeland 2006/2007*, pp. 135-39.

Those who have traveled by plane from certain airports in the United States in recent months may have undergone the straightforward process of explosives “sniffing.” This should become standard practice at all U.S. airports as quickly as possible. A national trace detector network would cost about \$250 million. Just as importantly, this country needs a comprehensive means of either screening cargo carried on airplanes or hardening aircraft cargo holds. And private aircraft are still insufficiently monitored. To prevent plane-based suicide attacks, there should be greater screening of private aircraft pilots by the federal government.

The threat to aircraft from surface-to-air missiles is real. Unfortunately, the technology to counter them is not yet ready for deployment. A sustained and serious R&D program is appropriate and might be expanded, but on this issue, available technology does not yet offer a good enough option to warrant the effort and expense of deployment. After a shutdown of a civilian aircraft, however, that assessment could quickly change.

The container trade is another area of major potential vulnerability. As with many issues considered above, perfect solutions are elusive, and brute-force methods of providing comprehensive security could be hugely expensive. But there are still practical steps that could be taken to substantially improve American security. Over the period 2001 to 2004 the number of cargo inspectors in the United States grew by 40 percent and the number of inspections by 60 percent. Even so, only 6 percent of seaborne cargo containers are inspected. To have a good chance of inspecting any suspicious container that is not being shipped by a company and port with strong security records, it would be safer according to informal conversations with experts to aim for inspecting 10 to 15

percent of all traffic. Over the longer term, a new type of system might provide positive confidence in virtually all containers—and such a system is now in use in Hong Kong.⁴⁶

As for state and local governments, in addition to the greater prevention efforts noted above, they do need the right kinds of improved consequence management capabilities. For example, a major city could purchase several dozen mobile interoperable communications systems, at a cost of perhaps \$1 million each, to facilitate communication between different first responders. The idea is that not every police radio need have the capacity to talk with every fire or rescue radio—but interfaces are needed that can go to the scene of an incident and facilitate the cross-communications that are required. Huge additional expenditures are not needed, but targeted additional investments make sense in such cases. Technologies are available, and procedures already have been tested, to make these interlinkages work (through some first responder communities, as well as the military's Joint Forces Command and Northern Command). But procurement practices need to be standardized and concrete plans need to be devised and implemented.

Since 9/11, as noted, key parts of the private sector have done relatively little to protect themselves. And Washington needs to spur them to do so. The role of the government is not to regulate onerous security standards everywhere, but to catalyze the private sector to protect itself. As suggested by Peter Orszag, an appealing approach would make use of the nation's insurance system, coupled with some minimal regulation of safety standards. By this concept, terrorism coverage would be mandatory on all commercial policies above some minimum threshold (such as several million dollars).

⁴⁶ Stephen E. Flynn and James M. Loy, "A Port in the Storm Over Dubai," *New York Times*, February 28, 2006, p. A19.

The government would play the role of a financial backstop, as indeed it already is given the renewal of the Terrorism Risk Insurance Act in 2005—but with the modifications that only extreme, catastrophic losses should be covered. A graduated rate structure in the insurance market, rather than government regulation, would then encourage best practices when there were affordable and reasonably effective.

As for some specific private sector initiatives: chemical and nuclear plants are potential targets for low-tech attacks with massive consequences. The U.S. chemical industry still has no legal framework guiding its security measures (which so far have been taken voluntarily). In this case, direct regulation is appropriate. Legislation to rectify this, including periodic safety assessments and common-sense solutions, should be a priority. There are also numerous cases where dangerous chemicals should be routed around large cities, and also where substitutes for them should be found when possible, as with chlorine for purifying water.

Nuclear power plants are now relatively well protected. However, areas where low-grade waste is stored are often not. This increases the likelihood of a radiological attack, and so the level of security must be improved.

Large buildings should have better security provisions too. Again, common sense, the use of the market, and a degree of patience can make such measures affordable. For example, when built or renovate, buildings should be fitted with air filtration and circulation systems that would minimize the permeation of chemical or biological agents. Other steps can be taken to protect buildings against bombs and infrastructure attacks, and should be reflected in new building codes. These could include elevators that descend to the nearest floor in the event of a power outage, building important buildings back

from roadways, using shatterproof glass in their lower floors, and controlling access for entry and for parking.

There is an important homeland security agenda that the next president and future leaders in the Congress will need to pursue. Some key vulnerable sites such as chemical plants are unprotected. So are most skyscrapers. Police forces in most cities have scant capacity to conduct counterterror work and depend excessively on a small national FBI capacity. Container shipping remains very lightly monitored; much air travel remains unsafe; international collaboration on homeland security has not progressed very far beyond sharing of names on terror watch lists. The progress we have seen to date has been significant, and the country has become much more secure. Yet a great deal remains to be done.