Cato Handbook for Policymakers

CATO INSTITUTE

7TH EDITION

47. Domestic Security

Policymakers should

- focus the federal government's efforts on the few areas where it can make a significant contribution to securing the country and eliminate federal security programs that are better performed by other levels of government and the private sector;
- make it clearer to the public that government homeland security efforts cannot make the country absolutely safe against possible terrorist attacks;
- ensure that homeland security efforts are not disproportionately focused on defending against the last attack, such as another 9/11 or the Madrid train bombings, at the expense of other vulnerabilities;
- avoid overreaction or exaggeration of the threat posed by terrorism; and
- ensure that civil liberties are not sacrificed for unneeded and ineffective homeland security measures.

In the wake of the terrorist attacks of September 11, 2001, the U.S. government asserted responsibility for much of the nation's domestic security by creating the Department of Homeland Security. The national government has important security responsibilities, of course, as epitomized by the constitutional power to ''provide for the common defense.'' But a single central authority cannot effectively secure a country as large, diverse, dynamic, and free as the United States. The job of domestic security has too many facets. Instead, the federal government should focus on the security issues that it is uniquely suited to address—the ones that states, localities, and the private sector cannot.

The threat of terrorism, which created the vogue for a national ''homeland security'' infrastructure, must be understood in a strategic context.

Terrorist attacks have direct costs, but they also seek self-injurious overreaction, such as the waste of blood and treasure on the part of the victim state; recruitment and sympathy gains when the victim state misdirects a violent response; and the weakening of the political order in the society attacked so that it is induced to act wrongly. When it does so, it cedes the moral and ideological high ground, making terrorists groups look relatively more legitimate. Policymakers should use risk management to prioritize security efforts, and they should avoid holding out the promise of perfect security, as there is no such thing. Civil liberties must be fully protected, and doing so is consistent with proportionate and well-focused domestic security efforts.

The Limited Federal Role in Domestic Security

The federal government has several important roles in securing against asymmetric threats like terrorism. But it is only one of many institutions arrayed against terrorism, and not the primary or only source of protection.

The federal government's strength is in its traditional international roles: setting a foreign policy that does not exacerbate grievances against the United States or legitimize the use of terrorism against us; developing intelligence information on international terrorist groups; and cooperating with and cajoling foreign governments to assist in pressuring and dismantling foreign terror cells. The federal government can aid state and local agencies that have responsibility for domestic security by disseminating relevant intelligence and vulnerability information within the country; by coordinating multijurisdictional counterterrorism efforts (just as it does with multijurisdictional crime); by maintaining a regularized border environment and interdicting known terrorists, weapons, and harmful materials there; and by providing information that helps state and local actors—public and private—prepare for and mitigate the effects of attacks or disasters.

The federal government cannot secure the thousands of bridges, sports stadiums, airports, bus stations, subways, and shopping malls, or the hundreds of skyscrapers, nuclear power plants, electrical substations, railway lines, food warehouses, water distribution systems, or telecommunications and computing facilities across the country. Responsibility for the security of internal infrastructure should be the responsibility of its owners and of local law enforcement. Since 9/11, the federal government has asserted roles in all these areas and more without regard to whether that level of

government is well-suited to the task or whether certain security measures even merit the expenditure of taxpayer dollars.

Use of Risk Management to Focus Security Efforts

The federal government response to the terror threat has been haphazard, oftentimes irrelevant, and occasionally counterproductive because it has been driven chiefly by politics. Instead of being reactive to past attacks and interest group demands, policymakers should focus the security efforts of all governments using risk management. The following questions illustrate a general risk management framework:

- **What are you trying to protect?** Every security program or technology is meant to protect some institution, infrastructure, process, person, or group that may be harmed.
- **What are you trying to protect it from?** Harm to the asset you are trying to protect can come in various ways. The goal here is to describe vulnerabilities and the relevant ways that an asset may be harmed.
- **What is the likelihood of each threat occurring and the consequence if it does?** Each threat has a different likelihood and consequence, and each factor may range from very low to very high. Risk assessment helps target limited resources efficiently by focusing attention on the threats with the greatest combined likelihood and consequence.
- **What kind of action is being taken in response to the threat?** There are four ways of responding to a threat:
  - — *Acceptance* of a threat is a rational alternative that is often chosen when the threat has low probability, low consequence, or both.
  - — *Prevention* is the alteration of the target or its circumstances to diminish the risk of something bad happening.
  - — *Interdiction* is any confrontation with, or influence exerted on, an attacker to eliminate or limit his or her ability to cause harm.
  - — *Mitigation* is preparation so that, should something bad happen, its consequences are reduced.
- **Does the response create new risks to the asset or others?** The final step in analyzing the program's efficacy is to be aware of new risks created by the prevention, interdiction, or mitigation of the threats under consideration.

These questions help illustrate why localized and decentralized security measures are most effective; a government that is trying to protect everything is protecting nothing. But they also show how the federal government can be helpful to the states, localities, and private-sector entities that actually secure the country.

Consider an example where one of the federal government's intelligence agencies picks up a plan to knock out electrical transmission facilities during a period of particularly cold or hot weather, which could threaten lives and cause economic disruption. This information can be passed along to the owners of the infrastructure so that they can step up the measures that physically secure their facilities (prevention). If the perpetrators are identified in any way, this information can be passed on to state and local law enforcement for possible interdiction. This threat intelligence can also be used to inform states, localities, businesses, and families about the importance of preparing for power loss (mitigation).

Avoidance of Wasteful and Counterproductive Overreaction

It is important to understand terrorism as a strategy. Like our foreign policy, our domestic security policy must be strategic. It must avoid the overreaction that terrorism seeks to engender. Terrorists often have great ambitions, but they lack the means to achieve their goals unless their intended target—be it the government of a nation-state or the citizens of that state—alters its behavior or adopts policies that otherwise redound to the terrorists' benefit.

As discussed in Chapter 46, ''Countering Terrorism,'' terrorism is violence typically used by weak, nonstate actors against states to raise the costs of the victim state's policies. A strong power victimized by terrorism will very likely do violence or take other responses that are badly directed, or even entirely misdirected. This reaction will tend to engender sympathy for the terrorists and aid in their recruiting and support. For example, Paddy Hillyard from Queen's University Belfast has articulated well how British responses to Irish Republican Army terror won sympathy and recruits for the IRA. Lashing out against the communities in which terrorists live, or the places where they hide, forces local neutrals into the wrong camp. And those neutrals are uniquely positioned to undermine those terrorists should they so choose.

Avoiding overreaction is essential for countering the strategic logic of terrorism. Indeed, it is the care given to the measurement of domestic security efforts that will help control terrorism. Huge U.S. government

spending on a vast repertoire of dubious security efforts since 2001 has put Osama bin Laden in a position to boast about the large returns on his small investment in the 9/11 attacks, and of his confidence that Americans will continue to expend resources in a vain attempt to chase down every potential terrorist. He crowed in 2004 that it is ''easy for us to provoke and bait this administration.'' Describing his desire to ''bleed America to the point of bankruptcy,'' bin Laden remarked, ''All that we have to do is to send two mujahedeen to the furthest point east to raise a piece of cloth on which is written 'al Qaeda,' in order to make generals race there to cause America to suffer human, economic and political losses.''

The haphazard and poorly coordinated responses of our federal domestic security agencies are no less a boon to al Qaeda. The Department of Homeland Security and the Transportation Security Administration are basically permanent multibillion-dollar drains on the public fisc. The REAL ID Act and Western Hemisphere Travel Initiative are similarly wasteful, self-destructive programs. These are just a few examples, and they were all prompted by a $500,000 al Qaeda investment.

The Threat to Civil Liberties

A terror-victim government can harm itself in other ways. Terrorists are battling for legitimacy. With little ability to build it on their own, they can at least degrade their opponent's. Terror attacks may cause otherwise liberal and tolerant societies to come somewhat loose from their moorings. Overreaction by the victim state erodes its claim of moral authority to rule; deviating from the rule of law, seeking extraordinary powers, and using mass surveillance all give terrorists legitimacy by admitting their power while undermining the legitimacy of an incumbent government by placing the state at odds with its people. By simply behaving well, the terror-victim government can deliver a devastating blow to terrorism because it causes the bad behavior of terrorists to dominate public perceptions.

In response to the events of 9/11, the Bush administration suspended, eroded, and ignored a range of civil liberties, all the while claiming such steps were legal on the grounds that they were necessary to prevent a future attack. In the course of implementing many of these policies, the Bush administration repeatedly asserted the ''state secrets'' privilege as grounds for the dismissal of civil cases that challenged the legality of its conduct in the war on terror, specifically with respect to two programs: the rendition of suspected terrorists to foreign countries for interrogation

purposes and the National Security Agency's warrantless wiretapping of communications by suspected terrorists.

The veil of secrecy should be lifted, and policymakers should act swiftly to redress civil liberties violations and restore rights that have been lost or diminished over the last several years. Immediate steps include banning trials before military tribunals, closing secret prison facilities, eliminating national security letters, denying authorities the power to jail citizens in the United States as ''enemy combatants,'' ending the practice of extraordinary rendition, banning torture, and ending warrantless wiretapping within the United States.

Emergency Preparedness

Part of avoiding overreaction is recognizing the hard truth: providing absolute and perfect defense against any and all future potential terrorist attacks is impossible. Though they are probably not as endlessly cunning as they are often portrayed, terrorists will bide their time and seek opportunities to stage dramatic attacks. All that can be expected of domestic security is to prevent what can be prevented and to recover well from what cannot. Policymakers who promise perfect security or the elimination of terrorist threats are committing leadership malpractice, just like policymakers who inflate the threat of terrorism.

The country must instead adopt a sound, comprehensive counterterrorism strategy. This begins with understanding terrorism as a strategy and with forcing policymakers to focus on securing the country against both the threat of attack and the threat of overreaction. The government should study how people perceive risk and how they overestimate dramatic but highly unlikely causes of death. A comprehensive counterterrorism strategy, which should include communications planning for reassuring the nation in the event of future attacks, will help ensure that the physical damage from any attack does not metastasize into undue damage to liberty or the economy.

Given the possibility of future attacks, the public should be educated about how to prepare for and respond to terrorist attacks, especially the potential use of chemical, biological, or radiological/nuclear weapons. These communications need not promote fear and could be blended into science curricula in high schools and colleges. Solid, science-based information should 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 the exaggerated assumptions about what such weapons can do should be debunked.

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 radioactive iodine from a dirty bomb), government officials can let people know exactly what they are, how they work, how to use them, and where to obtain them.

Put in the proper context, it becomes obvious that threat exaggeration is harmful behavior. Pandering to people's fear about terrorism should be a political liability. A public education campaign would force sound estimates of terrorists' capabilities to the surface. Currently, fantastical ''movie plot'' threats are assumed possible by far too many opinion leaders. Lacking information, they frighten Americans with scheme after scheme. Government authorities are free to cite only the ''intentions'' of whomever they prosecute, without reference to capability or to the technical feasibility of any plan. Sound threat assessment, therefore, is an essential part of domestic security.

Emergency Response

Emergency response to a terrorist attack (just as with a natural disaster) occurs at the local level. Therefore, instead of it being taxed away to Washington, a large chunk of the money authorized and appropriated for the Department of Homeland Security should be returned to taxpayers for their own use or for state and local response preparation.

Beyond easing public fears through an open, careful, and accurate discussion of threats, and beyond coordinating with state and local agencies, the federal government can take other active measures as part of a comprehensive and effective counterterrorism strategy. For example, there are uses for technology in defeating terrorism. But rather than focusing on mass surveillance, technology should be developed to speed the application of legal processes so that warrants for specific information, meeting legal standards, can be applied for, served, and responded to in short order. Better-organized responsibility for the security of the nation's infrastructure can ensure that knowledge and technology are applied smartly and cost-effectively to secure our infrastructure, to minimize damage should there be future attacks, and to heal injuries to our people and the organs of our society.

Many proposals ostensibly intended to advance domestic security, however, are unnecessary and counterproductive. For example, the United

States should not follow the ''English model'' by creating a domestic intelligence agency like MI5 and a new ''National Security Court System.'' A National ID card system—whether for ''internal enforcement'' of immigration law or any other reason—is similarly ill-conceived. Although packaged as an ''antiterrorism'' measure, determined terrorists will simply bypass the identity-based security system by either bribing the people who are supposed to check the cards or recruiting people with valid cards and ''clean'' backgrounds to carry out the attacks. And once the system is in place, it will be virtually impossible to dislodge as policymakers are loath to repeal laws and cancel programs—even where there is clear evidence of dysfunction or irrelevance. Thankfully, some states have taken steps to resist federal pressure to establish such a system because of the financial costs associated with implementation. It is disturbing, however, that the United States is still moving toward such a system with so little debate in Washington. Federal policymakers should reverse course and abandon the effort entirely.

Congress correctly responded to the popular backlash against the Bush administration's Total Information Awareness program in 2003 by eliminating the Pentagon office that was responsible for developing the suspect-tracking technology. Unfortunately, there are reports that the federal government seems to be pursuing the same software and other tools that could ''mine'' millions of public and private records for information about terrorist suspects in secret. If this is indeed the case, it raises disturbing questions not only about the merits of the TIA program itself, but, more generally, about the impervious nature of an emerging surveillance state, a state in which the bureaucracy, not the people, determine which policies will change and which will remain in place. Likewise, the federal government's long-term policy of DNA collection deserves close scrutiny. (For more, see Chapter 29, ''National ID Systems.'')

The federal government should preserve domestic security, generally, and respond to the problem posed by terrorism, specifically, from within the framework of a free society. In brief, that means having good intelligence, good civil defense, and focused police work. It does not mean secret prisons, torture, military trials, national ID cards, national security letters, secret arrests, suspension of habeas corpus, and warrantless wiretapping. The ultimate outcome is a political climate in which fearmongering is virtually absent and politicians engaging in such behavior are punished at the ballot box. This will occur naturally so long as there is a widespread political consensus on the nature of the threat and general agreement on the approach to that threat that assiduously avoids overreaction.

Suggested Readings

De Rugy, Veronique. ''Facts and Figures about Seven Years of Homeland Security Spending.'' Working Paper no. 08-02, Mercatus Center, George Mason University, March 2008.

Fallows, James. ''Success without Victory.'' *Atlantic Monthly*, January–February 2005.

Friedman, Benjamin. ''The Hidden Cost of Homeland Defense.'' *Audit of the Conventional Wisdom*, 05-12, MIT Center for International Studies, November 2005.

German, Mike. *Thinking Like a Terrorist: Insights of a Former FBI Undercover Agent*. Dulles, VA: Potomac Books, 2007.

Lustick, Ian S. *Trapped in the War on Terror.* Philadelphia: University of Pennsylvania Press, 2006.

Mueller, John. ''A False Sense of Insecurity.'' *Regulation* 27, no. 3 (2004).

Poole, Robert, and Jim Harper. ''Transportation Security Aggravation: Debating the Balance between Privacy and Safety in a Post-9/11 Aviation Industry.'' *Reason*, March 2005.

Shapiro, Jeremy. ''Managing Homeland Security: Develop a Threat-Based Strategy.'' *Opportunity 08*, Brookings Institution, February 2007.

Williams, Cindy. ''Strengthening Homeland Security: Reforming Planning and Resource Allocation.'' *2008 Presidential Transition Series*, IBM Center for the Business of Government, Massachusetts Institute of Technology, 2008.

—Prepared by Jim Harper and Christopher Preble