

Forthcoming in Stephen Maurer, ed., *WMD Terrorism: Science and Policy Choices* (title provisional), MIT Press, 2008. PLEASE DO NOT CITE OR QUOTE WITHOUT PERMISSION.

8 Weapons of Mass Destruction: Are Our

Political Institutions Adapting?

Eugene Bardach, Goldman School of Public Policy,
University of California at Berkeley

Just because the WMD threat is urgent, consequential, and novel does not mean that our policy institutions' responses will be immediate, effective, and creative. In some respects, these institutions are just not well suited to the task. Public sector bureaucracies move slowly and are bound by established procedures; and the complex nature of the threat demands an unusual level of interagency, intergovernmental, and inter-sectoral cooperation. More importantly, the WMD problem itself is much larger than the sort of problem government must ordinarily deal with. Even if all policy-makers were wise and full of understanding, and even if all implementing institutions were nimble and clever, we would still have to struggle.

Our policy institutions must do the best they can, though – indeed, better than usual. Are they measuring up? It is not possible to unambiguously answer this question. For example, if we try to evaluate efforts to prevent attacks (mostly intelligence-oriented and military approaches), we have no way of observing and quantifying attacks that did not occur. Even if estimates were somehow possible, we still cannot say what bearing our explicit efforts have on the outcome.¹

In this chapter I take a more indirect approach. I consider not performance but adaptive capacity. I consider five elements of adaptive capacity in our institutional system, and I ask whether there is reason to think these are currently effective and cost-efficient or are moving on a reasonable trajectory in these directions. They are:

- mobilizing sufficient resources
- expending resources wisely
- involving the private sector
- creating and improving institutional capacity
- governmental learning

My conceptions of effectiveness and a “reasonable trajectory” are framed in large part by what I take to be how our policy institutions adapt in general to the full array of public problems. Because my sense is that our institutions

generally perform in some middling way – not terribly, but certainly nowhere near a theoretical optimum – I look particularly hard for evidence that, in the WMD case, with its high stakes and severe technical challenges, our institutions might be doing **better** than they usually do.

I do not claim that these five elements of institutional capacity are the only important aspects of societal adaptation or that they derive from any widely accepted theory of process.² They do seem reasonably important, however. They also happen to link to phenomena such as budgeting, regulating, reorganizing, and getting bureaucracies to work collaboratively that are already familiar and reasonably well studied in political science and public management.

8.1 Counter-WMD and Counter-Terrorism

At the outset, let me state an assumption about the relationship between strategies aimed at terrorism in general and those aimed at WMD in particular. Often, there is so much overlap that, for many purposes, it is not worthwhile distinguishing them. For instance, most intelligence strategies against terrorism are resourced and managed generically. Even strategies aimed at particular WMD activities, such as exposing nuclear smuggling or bioweapons laboratories, are probably not very different from intelligence strategies more generally. The same applies to the

interdiction of weapons and potential weapons materials, and to the hardening of potential targets.

On the other hand, the distinction between WMD and other forms of terrorism is very important for consequence management. A successful WMD attack amounts to a catastrophe. Unlike mere disasters, a catastrophe has vast impact and significantly erodes organized response and recovery capability, such as communications, preexisting plans, and critical infrastructure. (Quarantelli 2006) September 11 was a disaster, a huge disaster to be sure, but not a catastrophe. Hurricane Katrina, in contrast, was a catastrophe. Blowing up the White House would be a disaster for national morale, but not a catastrophe. A nuclear bomb detonated in Manhattan would be a catastrophe, with hundreds of thousands dead, and perhaps even more than this seriously injured. (Allison 2004)

We need to think differently about catastrophe than we do about disaster. In particular, we need to think about how to write off cherished communities and places, or at least to consider doing so. Although in some quarters it is unacceptable to say so, using federal tax dollars to rebuild New Orleans to its previous state is not the obviously moral and practical thing to do. The distinction between catastrophe and disaster can also sharpen our sense of what exactly

counts as WMD. A bundle of conventional explosives could count as WMD if they destroyed a tunnel that played a critical role in a regional economy.³

Another area in which the catastrophe/disaster distinction matters is resource allocation. For current levels of financial and organizational investment, the returns to preventing catastrophes are probably higher than mitigating them, although both investments are probably worthwhile. The organizational investment – particularly in the intelligence agencies – is particularly problematic, and I shall discuss this in detail below.

Data and sources. The reader must pardon another throat-clearing preliminary, this one about the data that figure in my discussion. The mobilization to counter the WMD threat is far-ranging, complex, varied, and to some degree concealed. Roughly 50,000 agencies are involved at all levels of government, ranging from the CIA and FBI at the federal level down to fire and public health departments in cities, towns, and hamlets. The strategies range from penetration of suspect Islamist groups in Germany to the installation of pathogen sensors in Chicago. The most informative sources of information about this ocean of activity are government reports and hearings (e.g., by the Government Accountability Office), reports in the quality press, writings by former government officials, and the analyses of security intellectuals in think tanks. There is only a scant academic

literature assessing the nature and effectiveness of such operations, and much of this literature is based on such governmental and journalistic sources in any case. I have myself done almost no original research but have relied on existing sources.

That these sources may not accurately represent the vastness and complexity of the nation's collective effort almost goes without saying. But is the admittedly imperfect representation also a biased one? I think it is, in three important respects. First, there is a tendency to report bad news rather than good, especially in the accounts of journalists and former officials. (The wary reader can offset the self-serving bias in some of these accounts to some degree.) My own selection of examples may have been biased in this way as well, partly because I have become skeptical after many years of studying policy-making and implementation. To offset this bias, I tried to find examples of adaptive success. Secondly, the selection of data and their interpretation are almost surely skewed towards emphasizing the importance of individual competency and motivation and downplaying institutional or systemic factors. I do not at all discount the role of individuals, especially as potential antidotes to some systemic pathologies, but my goal is to rebalance the prevalent perception. The policy system's successes (troubles) coping with the WMD threat are best understood as a variant of its successes (troubles) coping with the broader problems of modern life. Thirdly,

most of the non-academic literature does not attempt to assess trade-offs, to compare, even approximately, costs and benefits. If data mining violates privacy, for instance, in some quarters this is taken to be an absolute bad and the benefits of the violation are assumed to be trivial by comparison – or vice versa. I shall at least try to assess how well the system balances costs and benefits.

8.2 Mobilizing Sufficient Resources

In times of crisis, it is easy for the federal government to throw money at problems. Although budgetary commitments to past and present priorities weigh strongly against change, the federal budget is large and some reallocation is possible. More importantly by far, though, is the ability of the federal government to engage in deficit spending, a power denied to most state and local governments. It can thus respond to new situations very rapidly, without the long and politically tortuous process of increasing taxes and fees or issuing bonds. In the six years preceding September 11, federal spending on domestic security increased from \$9 billion to \$16 billion. But in the year following September 11, the federal government added emergency supplemental appropriations of about \$21 billion. (Carafano 2007) With some blips, federal spending continued on its dramatic upward course, from \$15 billion prior to September 11 to \$42 billion in 2007, according to estimates by scholars from the Brookings Institution.

(O'Hanlon 2006)⁴ State, local, and private expenditures appear to have been relatively modest.⁵

There is, of course, the question of whether this growth is too much or too little. What forces might be causing us to over- or under-spend?

8.2.1 Too Little, Too Slowly

Suppose, for the sake of discussion, that we are doing too little too slowly, an assumption supported by a broad ideological consensus among most security intellectuals. The liberal-centrist Brookings group argues that “much more needs to be done” but adds that “enormously expensive measures” are not “necessary or appropriate at this time.” They recommend add-ons to federal spending for 2007 of \$10-20 billion and private sector additional spending at a “roughly comparable” amount. Similarly, a group of public figures and terrorist experts issued a report for the liberal Century Foundation in 2006, which claims that our post-September 11 response “undeniably has had an overseas emphasis” (meaning primarily Iraq) and proposes measures that would add an estimated \$23 billion to an administration budget request of \$50 billion. (Beers and Clarke, 2006) Philip J. Crowley, of the liberal Center for American Progress, in an overall assessment of homeland security policy in January 2007 recommends fourteen steps to improve homeland security at an estimated cost of \$12 billion to

\$18 billion. (Crowley, 2007)⁶ On the farther left, at least some voices are worried about underinvestment in homeland security. In their September/October 2004 issue, *Mother Jones* published an essay by Matthew Brzezinski that called the Department of Homeland Security “badly underfunded.”⁷ On the right, James Jay Carafano, the principal homeland security analyst at the Heritage Foundation, also proposes a long list of measures and projects that seem urgent and expensive. (Carafano, 2007)

If we are spending too little too slowly, what might be the reasons? One possibility is that there is limited “absorptive capacity” at the level of actual implementation. If tomorrow you were to be given \$100,000 by your local government, say, to make your own suburban residential neighborhood safer, you would probably have trouble knowing exactly what to do with it. You would probably wish to establish priorities based on cost-effectiveness calculations, but you would then need to face the divisive issue of how much safer against what kind of threats. You would also need to search for and contract with appropriate contractors, establish government-approved accounting and documentation systems, and design safeguards against being steamrolled by local demagogues or wheedled by individuals with pet projects. As Carafano observes, the federal budget for FY 2004 actually decreased security spending relative to FY 2003, when the budget included many one-time costs and when “allowing the many

agencies involved some time to absorb the large increases since September 11...”
(Carafano 2007)

The politics of the budget process, along with its procedures, also play a role. The budget process in all large organizations, and especially in government, is conservative. It is designed to handle growth and change, but incrementally and not in leaps. For a year or two after a crisis or some other dramatic anomaly, the discourse about budgetary requests might be dominated by talk about problems and responses. But it will not be long before the discourse is drawn back to its natural state of “what you got last year” and “the increase you’re asking for this year.” Furthermore, increments, not problems and solutions, are the natural medium for perception as well as discussion. An increment in domestic security spending of some 200% from 2001 to 2007, or \$15 billion to \$42 billion (according to the Brookings figures above), just seems like a lot in the eyes of those officials playing the federal budget game across the agencies, the President’s Office of Management and Budget (OMB), and the Congress.⁸ It seems especially a lot in the absence of successful terrorist attacks on US soil since September 11. For these professionals, steeped in the customs and conventions of the budgetary game, increments of seven or eight percent generally seem large.

Another possibility is one variant of what economists call fiscal illusion, that, at the margin, spending tax dollars is all cost and no benefit. (Downs 1960)⁹ It affects primarily two kinds of people in the political class: ideological conservatives, whose overweening concern for tax dollars is offered as an offset to liberals' presumed relative indifference to them; and political figures of all stripes who find it very painful to solve the problem of where, exactly, the money is to come from. It is indicative that in the published version of James Jay Carafano's Heritage Foundation lecture on "Homeland Security Spending for the Long War" (Carafano 2007), the third of his three main (bulleted) points concerned the long-term growth of entitlement spending (Social Security, Medicare, and Medicaid primarily) which he sees as a direct competitor for homeland security resources.¹⁰ On the politically liberal side of the aisle, it is the "offensive component" homeland security – that is, the Department of Defense – and the Iraq war that are seen as the main culprits out-competing homeland security needs. (Beers and Clarke, 2006; Crowley 2007)

There may be political incentives, in most jurisdictions, to give lower priority to costly counter-terrorism measures than would be optimal. Owing to several expert analyses available to the US Congress, the US Army Corps of Engineers, the civil engineering community, and the White House, the levee systems in New Orleans, prior to Hurricane Katrina, were known to be inadequate

– the Federal Emergency Management Agency (FEMA) ranked them the #3 hazard nationwide – but expensive to upgrade. From the perspective of elected officials it is often better to play the lottery and hope that such expenses can, without adverse consequences, be deferred till after they have left office. This gamble often works because the political time-horizons of elected officials are usually shorter than the average expected-time-to-disaster.¹¹ The same logic applies to counter-terrorism planning, except possibly for very salient targets such as New York City or Washington DC.¹²

This scanting of the long-term can be somewhat offset by counter-terrorism-related investments that serve other purposes as well. The “all-hazards” approach to catastrophe and disaster planning, which aims to manage generic consequences rather than the full array of differential consequences attributable to different causes (earthquake, WMD attack, chlorine gas plume), is by now the dominant approach to emergency planning, and so embodies this principle. However, as many observers have remarked, catastrophe and disaster planning are policy areas without much of a political constituency to begin with. (Birkland 2006)

So far we have been explaining spending “too little too slowly” at the systemic level – budget routines, electoral incentives, absorptive capacity. But we

should also look in a finer-grained way at the particular problems afflicting particular programs and projects. One problem stands out: Homeland security issues are often nested in a larger set of problems that are themselves contentious and take a long time to resolve. Here are some examples:

- Improving carry-on inspections at airports following September 11 was caught up in the larger issue of privatization of government functions. The Administration was reluctant to take on an extra 45,000 or so civil servants and made an ideological point about the benefits of outsourcing, and the Democrats in Congress made their own stand in opposition.
- Following a catastrophic event, the need for rapid and well-targeted communications among first responders is obvious. The Federal Communications Commission (FCC), which has been the central government actor in assigning frequencies and creating technical standards, has assimilated the emergency inter-operability problem to its normal, and slow, deliberative processes. These processes have had to accommodate many parties with different interests, ranging from private sector manufacturers to public sector emergency services agencies that differed among themselves on such matters as backward

compatibility and the need for expensive equipment replacement programs. (Mayer-Schonberger 2003)¹³

- The question of who should pay bedevils many policy choices in the domestic security area. Because in some cases so many parties benefit from security expenditures, cost-sharing arrangements are in principle logical and just; but they may be contentious when it comes to specifics. Consider, for instance, that any WMD attack – an anthrax bomb going off in Chicago, say – is likely to be aimed not merely at a physical target but at the morale and the economy of the entire nation. Preventing such an attack benefits primarily Chicagoans but also residents of Keokuk, Iowa and Bakersfield, California. Some sort of federal subsidy is warranted in this case, but how much?¹⁴

And in the case of interoperable communications equipment, the case would be further complicated by the fact that emergency communications are traditionally a local responsibility. A federal subsidy might induce some to come aboard the interoperability train but others, who might have recently purchased new equipment, or equipment incompatible with the new standard, might need to be mandated. But does the federal government have the right to impose such a

mandate? And if it does so, should an accompanying subsidy take account of the costs recently incurred by the city's equipment upgrade?

- The Cooperative Threat Reduction program, begun in 1992 as the Nunn-Lugar program, subsidizes efforts by Russia and other states of the former Soviet Union to destroy or secure thousands of “loose nukes” and other WMD. By all accounts, it has been very successful so far but, as of November 2005, had finished only about half the task. (Public Discourse Project, 2005a) Over the years it has run into a lot of trouble, some substantive, such as Russia's refusal to grant access to certain sites, but some originating in ancillary concerns, such as corruption, distaste for supplying make-work jobs to underpaid Soviet military scientists (to divert them from working for rogue states or terrorist organizations), and a suspicion that we were somehow being made fools of. (Kelly, 1996)
- At any implementation site, specific, and often unforeseen, problems may arise that delay or distort implementation. At six southern US border sites, the installation of radiation-detection

portals was delayed in order to mesh with the sites' expansion activities. (GAO, 2006a)

This cross-hatching of policy issues, policy decisions, and policy arenas is mainly due to the sheer complexity and scope of problems and their solutions. It is also due to the nature of American government, with its traditions of federalism, separation of powers, and fragmented political parties. This system normally prevents policy-makers from taking speedy, coherent, and large-scale action, whether those would likely turn out as regrettable mistakes or as highly beneficial social adaptations.

8.2.2 Too much, too fast

At the farther edges of the political spectrum, both right and left suspect we give too high a priority to homeland security. On the right, the big cost is in wasted dollars and, on the left, ethnic discrimination. Both sides tend to be less concerned about the loss of civil liberties and invasions of privacy.

The critique here has two primary components: there is no point paying for perfect safety, which is unachievable in any case; and, though WMD are worth worrying about, Al Qaeda and its offspring have little capacity to manage their initiation and/or delivery. And in the case of the most articulate and

sophisticated of the critics, Ohio State University Political Science professor John Mueller, very few Islamist terrorists are on American soil anyway. But if this is the situation, why have we failed to see it? Why have we, in effect, over-adapted?

Explanations differ depending on one's politics. For the libertarian right, such as the Cato Institute, the "war on terror" is yet another manifestation of the tendencies of politicians and bureaucracies to aggrandize themselves at the expense of civil society. Mueller's generally libertarian critique argues that a "terrorism industry" is responsible for the "obsessive focus on terrorism" after September 11. This is an industry pursuing "the profits of doom" and consisting of "various risk entrepreneurs and bureaucrats, ...most of the media and nearly all politicians."

Some elements of the liberal left think that we are spending too little too slowly, and are happy to criticize the government for this fault. But other elements share the skepticism of the libertarian right, although their reasons are different. The reasons are in a sense partisan, albeit not closely tied to party: they emphasize what it takes to be the us-against-them foreign policy worldview of the Bush administration, the "neocons," and the more visible representatives of this outlook in high office, e.g., the President himself, Vice-President Cheney, former Defense Secretary Donald Rumsfeld.

These critiques are generally served up with a sprinkling of cynicism. But one need not be a cynic to suppose that when politicians are campaigning for election or reelection they will emphasize the issues on which they think they have a comparative advantage. In the three national elections since September 11 and up to this writing, polls have shown that the Republicans have been more trusted to protect the country from terrorism. (American Enterprise Institute, 2007) In national polls in September 2004, President Bush was rated as better able to “handle terrorism” than John Kerry by almost a 2-1 margin. (Pew Research Center, 2004) As public opinion has drifted away from the Republicans on Iraq, the privatization of social security, and environmental protection, one need not be a cynic to understand why they have tried to magnify their significance as warriors against terrorism. As to agency officials with a homeland security mission, and vendors and technologists who might profit from selling their security services or wares, these interests are no different from those that populate any other policy sector. It would be surprising if most individuals in these lines of work did not genuinely believe in the terrorist threat and the value of persuading others to share their views.

8.2.3 Just right?

The “too little too slowly” critique seems to me to have the better part of the argument. Mueller makes much of the fact that international terrorism “kills a few hundred people a year worldwide – not much more, usually, than the number who drown yearly in bathtubs in the United States” and that the global probability of death by terrorism, 1 in 80,000, is about the same as being killed by the impact of an asteroid or comet. But WMD attacks would be catastrophic, not merely disastrous, terrorism; and the probabilities of death would be much higher in the cities likely to be targeted (e.g., New York, Chicago, London). Also, the psychological and economic impacts of successful attacks could be immense, far worse than September 11 or Katrina. The economic losses could mount to the low trillions of dollars. (Bunn, 2006) Moreover, the idea that it is very difficult to create a workable and concealable nuclear device or a potent and dispersible bioagent is of small comfort if you take the long view, say, 20-30 years. Terrorists make mistakes, they learn, they practice, they fail, they try again...¹⁵ The roots of our problem lie in our technology, which packs more lethality into ever-shrinking and ever more accessible vessels, and in our desires for an open society. Those things will not soon change; therefore, neither will the threat.

Unfortunately, appropriate investment in our preparedness and vigilance will – should be – tied to this chronic situation as far ahead as we can see, which is not very far and, in any case, through an emotional as well as a cognitive haze.

Psychologically, most people substantially underestimate the likelihood of extreme events, such as very powerful earthquakes or floods or hurricanes (Berger et al., 2006). Their ability to think probabilistically is limited and in any case costly. (Kunreuther and Pauly, 2004) Underestimation may also avoid unpleasant realities. On the other hand, people have been telling alarmist stories about terrorists and various forms of WMD since World War II and in some cases even earlier. In retrospect, it is reasonable to think that those estimates were driven at least as much by psychology and culture as by any actual threat. We might not be able to reason with any greater clarity, whatever the direction we end up choosing.¹⁶

8.3 Spending the Resources Wisely

Does government spend its money wisely, that is, on the right things? No doubt governments make plenty of mistakes and waste billions. Nevertheless, some perspective is necessary. The sources of waste are diverse, and some are more forgivable than others.

Consider one of the more contentious spending programs, one often mocked from all political quarters, the State Homeland Security Grant Programs (SHSGP), which provides grant-in-aid programs to state and local government for

first responders, critical infrastructure protection, mass transit systems, and port security. From FY 2001 to FY 2006, the first responder funding went from \$616 million to \$3.36 billion. (de Ruyg, 2005) There is a good public-finance rationale for such a grant-in-aid program if it is allocated according to risk and the risk factors include being a target with national significance, for symbolic or economic reasons. An attack on the Golden Gate Bridge is to some degree a symbolic attack on all America; the country as a whole should contribute to protecting it and, in the event of its destruction, to mitigating the effects and perhaps to rebuilding it. The same could be said of many other targets, including whole metropolitan areas that might come in for WMD attacks.

The divergence of allocations from risk-based principles, however, has given the program the flavor of pork. (Roberts 2005) In the initial years, the allocation formula required minimum spending in each state, which meant that a sparsely populated state like Wyoming would receive \$17.5 million in FY 2004. A population-based factor in the allocation formula also skewed money away from the highest-risk locales. More recently, and following much protest from the higher-risk cities and states, the allocation formula was revised to favor larger and riskier urban areas, although no extra weight is given for region of the country. (GAO, 2007b; Hsu and Sheridan 2007)

States pass most of the money along to localities (by law at least 80%), and here too technical rationality sometimes takes a back seat :

- \$63,000 on a decontamination suit put in storage in rural Washington State because the state did not have a HAZMAT team to use it. (de Ruyg 2005)
- \$30,000 for Lake County, Tennessee, for a defibrillator to be kept as a standby at basketball games by a local high school. (de Ruyg 2005)
- \$557,400 to North Pole, Alaska, for rescue and communications equipment. (de Ruyg 2005)
- \$500,000 to Outagamie County, Wisconsin for chemical suits, generators, rescue saws, and a bomb disposal vehicle, among other items. (de Ruyg 2005)
- Yuba City, California, which was not even on the state's list of priority targets, bulletproofed its police station lobby and installed a 10-foot-deep barrier of steel-reinforced concrete pilings to halt vehicle intent on ramming the building.
- The agriculture commissioner of Stanislaus County, California, bought a database that federal authorities listed as a tool for intelligence gathering

but that he uses to keep track of what the county's farmers are growing and the pesticides that they use.

As often happens in federal grant programs, the logic of giving flexibility to state and local officials, "who are closest to the problems," runs up against the logic of ensuring that the problems they choose to solve, and the means used to do so, reflect federal policy. (Seidman and Gilmour 1986; Agranoff 1989; Oates 1972) It also runs up against the transaction costs and micromanagement needed to prevent these inappropriate expenditures.

Besides classic government waste and classic pork barrel politics (Olson 1982; Glazer and Rothenberg 2001), there is probably another element to the wide disbursement of funds in this context. It is the political reluctance to seem to be saying "Your community has too little of value to be a likely target" and/or "If you are hit, we don't care as much about your lives and wellbeing as we do about other people's." A journalist writing in the *New York Times Magazine* reported that officials talked about "relative worth and the right of [small state] citizens to get the same kind of protection that they are afforded in other places in the country," as though "same" need not take account of differential likelihoods of being targeted. (de Rugy, 2005)

Tales of pork show up particularly often in critiques from the political right. However, by the standards of federal spending in general, or of conventional pork barrel politics, these are small sums. If even half of all expenditures for state and local assistance were a complete waste, the loss would be only 2-3% of total spending on homeland security. Moreover, behind-the-scenes agreements by influential Congressmen and Senators, reached at the time DHS was created, have by and large kept DHS appropriations bills remarkably free of pork-flavored “earmarks.” The rationale was that homeland security was too important to be subjected to all the distortions of domestic politics, although the earmarking trend has been slightly upward from 2004 to 2006. (Basich 2006)

Other forms of waste are more debatable, and illustrate the difficulty of defining the concept in this area. Very large expenditures on counter-measures are often worthwhile if they actually work and the threat and risk are great. But this calculation often depends on subtle estimates such as the likelihood of a complex response system actually working in the event it has to do so; the ease with which the counter-measure can be defeated, either now or in the foreseeable future, by either (1) amateurs and semi-competents or (2) professionals and highly skilled individuals; and the rate of false alarms that occur due to imperfect detection and/or interpretation. Observers can differ greatly on such estimates. What looks like a reasonable and prudent investment to one person can look to another like

preposterous and irresponsible waste of resources. The flip side of this is that what looks like clear-sighted economizing to one person looks to another like callous indifference to life and playing dice with the nation's economy and morale.

A broader question is how best to allocate aggregate spending across prevention, mitigation, preparedness, response, and recovery. With regard to natural disasters, many experts tend to see higher social returns for investment in mitigation than preparedness and response. But the political incentives favor expenditures on preparedness and response, particularly ex-post assistance and relief in the immediate aftermath of an event, with almost no attention to spending the resources in ways that mitigate future vulnerabilities. (Birkland 2006) This dynamic will probably not affect mitigation investments in regard to terrorism, although other dynamics – such as electoral-cycle short-sightedness – may do so. But it appears that there is excessive federal attentiveness to supporting local first-responders as opposed to local capacity for intelligence-gathering and information-sharing. (Carafano and Rosenzweig 2005)

Crash spending. Homeland defense, in the post-September 11 world, has amounted to a crash-spending program. As with all crash spending, moving money out the door in a generally desirable direction is more important than

getting the details right. Given the urgency of responding to a threat, this is a sensible social adaptation. Some waste can, and should, be tolerated, especially as the technology of counter-measures, and of terrorist attack strategies, is in continual flux. Whether the waste has been excessive even by these relaxed standards is a legitimate question as well, however, although a question that is difficult to answer.

Consider the decision by the Domestic Nuclear Detection Office (DNDO) in the DHS, in July 2006, to award contracts to three vendors to further develop and purchase \$1.2 billion worth of cargo screening equipment over five years. The decision to move ahead on advanced spectroscopic portal monitors (ASPs) contracts was not uncontested. Since 2003, the GAO, at least, had been questioning the ability of Customs and Border Patrol (CBP) – prior to the creation of DNDO in 2005 the responsible agency within DHS – to deploy inspection portals effectively. (GAO, 2006b) Some months before the July 2006 contracting decision, the GAO, growing ever more skeptical of the ASP technology, requested that DNDO carry out a cost-benefit analysis. The results of the analysis, delivered in May 2006, might have convinced DNDO to move forward, but it did not convince GAO. The DNDO had set a performance requirement of 95% reliability in identifying highly enriched uranium (HEU) when it was present, but the technical assessment showed that the prototypes, from three different

manufacturers, could detect unmasked HEU only 70-88% of the time. The DNDO told the GAO that they were counting on substantial improvement in the ASP technology in the future, “but they provided no additional information as to how the 95 percent performance goal will be achieved or an estimate of when the technology will attain this level.” (GAO, 2007c)¹⁷

Perhaps the most charitable interpretation of this sequence of events is that the Office was realistically banking on technical improvements and that the risk of their being somewhat overly optimistic on that head was not as bad as the risk of leaving containers unsecured until greater certainty, if not better technology, were to emerge. However, even if that were the case, my point about the negative impact of crash programs still holds. Being overly optimistic, even if justified, is still being something less than realistic.

8.4 Involving the Private Sector

Running intelligence and law-enforcement operations are obviously public-sector responsibilities. So too are protecting public monuments, managing evacuations, and mounting military operations against terrorist training camps abroad. But the private sector has a critical role to play as well. Some 85% of what DHS calls “critical infrastructure” is privately owned, e.g., energy generation and transmission, cyber hardware and software, financial institutions, telecommunications, chemical production and storage and transportation facilities. A successful attack on such infrastructure could have ramifications well beyond the loss to the owners; and the owners would not necessarily take account of these when they decide how much to invest in protecting them or to restoring them to service following the attack. Regulation is probably the main governmental approach to inducing private owners to confront the possibility of these additional damages. In addition, it is the private sector that manages most of the R&D capacity in the economy. Since this capacity must be harnessed to counter-terrorism objectives, and private markets often fail to internalize security risks, government needs to step in somehow.

8.4.1 Regulating

Government acts not only by spending money directly but by mandating that private parties do so as well, e.g., by setting security standards for shippers or hazardous facilities and enforcing compliance. As a governmental problem-solving strategy, regulation has at least one big advantage compared to direct spending: it circumvents the constraints and the distortions and the politics of the budgetary process. In doing so, however, it runs into the constraints and the distortions and the politics of the regulatory process.

Consider first the possible distortions. The world is heterogeneous whereas regulatory standards tend to be uniform. Exceptions are always made, to be sure, but they can rarely keep up with the true variety in the world. And the more exceptions, the greater the complexity. And the greater the complexity, the greater potential for litigation, delay, frustration, and injustice. Some objects of regulation, therefore, will be regulated too strictly and others too leniently. (Bardach and Kagan, 2002; Tietenberg, 2006) Of the approximately 15,000 facilities in the United States that use hazardous chemicals, for instance, over 100 could endanger more than a million people if an explosion were to discharge plumes of toxic or flammable gas (or liquid) into the environment if weather and other conditions were right. (Marek, 2006) But until DHS issued a regulatory rule in April 2007, security regulation of chemical plants was so lenient that the most hazardous were not controlled much more tightly than the least hazardous.¹⁸

Using its political influence, the chemical industry was able to fend off appropriate regulation until April 2007, aided until January 2007 by Republican control of the White House and the Congress. This fits the usual pattern of regulatory politics, in which self-conscious “concentrated interests” facing compliance costs are better able and more willing to organize in opposition than aggregations of beneficiaries who, taken one at a time, would get very small payoffs. (Weimer and Vining, 2005)

Politics also enters into the question of state and federal regulatory roles. Concerning “social regulation” (e.g., health, safety, environmental protection, anti-discrimination, consumer protection), the federal government is generally stricter than the states, largely because consumer groups are better represented in Washington than in state capitals. Producer groups, therefore, usually prefer state regulation, while consumer groups look to Washington and argue for federal preemption. But sometimes the situation is reversed, and chemical plant security is a case in point. New Jersey, for instance, home to 140 major chemical facilities, adopted a fairly stringent set of regulations in late 2005 and has been resisting federal preemption provisions in bills moving through the US Congress. The DHS rule of April 2007 explicitly permits additional regulation by the states.

Regulating creatively. Managed creatively, regulation can be used to reward desired behavior and discourage or punish what is not desired. Under the Customs Trade Partnership Against Terrorism program (C-TPAT) Customs and Border Patrol (CBP) offer expedited and fewer inspections to shippers who voluntarily comply with CBP security guidelines and adopt a menu of “best practices” for securing their supply chains. To attract shippers into C-TPAT, CBP stresses the business value of increased protection against theft and the overall improvements in supply chain efficiency. But it stresses even more the cost-savings (for “validated partners”) from a reduction in the number of random inspections, eligibility for access to FAST lanes at the Mexican and Canadian borders, consultations from CBP supply chain specialists on regulatory issues, and other benefits under CBP control. (CBP, 2004b)

On paper, as a piece of regulatory program design, C-TPAT is excellent. It is results-oriented, flexible, fair-minded, and aims to minimize compliance and transaction costs while improving security. As with much regulation, however, the devil is in the details of implementation. For a period of several years, the monitoring regime in practice was too slack. The GAO issued a critical report in July 2003 noting that shippers received the benefits of reduced scrutiny simply for agreeing to participate in the program and without having their security profiles reviewed. (GAO, 2003b) Two years later, there was still very little monitoring of

private partners' actual behavior once they had been accepted. And even monitoring that appropriate security systems were in place – “validation” – was done haphazardly and without formal protocols. (GAO, 2005a)

The Achilles' heel in this otherwise well-designed government program seems to have been insufficient staffing, a common public-sector problem. CBP initially set a goal of validating all companies within three years following certification, but this proved impossible. CBP needed vastly more personnel possessing the specialized skills needed to evaluate supply chain security. The C-TPAT budget has increased substantially in recent years, as has its staffing; and it has committed itself to validate newly certified partners within one year and revalidate existing partners every four years. But the rapid increase in membership threatens these ambitious goals. (Caldwell, 2007)

Government reliance on industry for self-enforcement is not the only way in which government can leverage industry effort. Government also relies on industry to come up with standards, best practices, norms, and education strategies. As noted above, DHS appears to be doing something like this with planning councils made up of more-or-less representative owners of critical private infrastructure. There are fifteen such sector-based councils, each of which interacts with councils of government agencies focused on the same sectors. The

GAO reported in March 2007 that all but one of these councils had submitted their infrastructure protection plans. (Larence and Powner 2007)

It remains to be seen, of course, whether these plans turn into appropriate action. The delays in developing regulations for the chemical sector, which arose primarily from the industry side, raise concerns. The DHS has also been the source of delays. It did not publish its final version of the planning framework, the National Infrastructure Protection Plan, until June 2006, and after several false starts.¹⁹ The Century Fund's critique of progress in this area pointedly emphasized DHS's failure to stipulate outcomes and goals and to clarify industry's responsibilities. (Beers and Clarke, 2006) This has been a fairly common problem in government, though progress has been made in recent years at the federal level, particularly by means of management practices imposed in the course of budget reviews by the Office of Management and Budget.²⁰

8.4.2 Stimulating Private Sector R&D

The DHS in FY 2007 will spend just short of \$1 billion on R&D. Spending on threats from WMD is the topmost priority, particularly radiological and nuclear threats (almost a third). (AAAS, 2007) Most of these funds are spent in the private for-profit and non-profit sectors (including several university-based "Centers of Excellence"), although substantial amounts also go for government facilities such

as the National Biodefense Analysis and Countermeasures Center, which is being constructed. The US Government is currently in the process of spending \$5.6 billion on private sector research and vaccine production under the auspices of Project BioShield. The intention is to stockpile medicines that might be of use in the event of a bioterror attack. Many other such programs could also be mentioned, in the Department of Defense, the Department of Energy, the CIA, etc.

How effective are government's efforts to stimulate the needed R&D? Again, one must be cautious in answering this question, and the closely related question of how cost-effective such efforts are. No doubt the failures and imperfections draw more attention from the GAO and from outside critics than do the successes. That said, however, one's impressions are not, on the whole, reassuring. Project BioShield, authorized in mid-2004, has produced very little of value so far. Some of the reasons are technical: vaccines can fail in many different ways and production cycles are normally lengthy. But other reasons are institutional. Executive-branch policy-makers failed to change course even when a contract of \$877 million to develop and produce 75 million doses of anthrax vaccine attracted only one serious bidder, VaxGen, a small company with a track record of no successes and one failure (an AIDS vaccine). (Lipton, 2006) Moreover, the Office of the Assistant Secretary for Preparedness and Response,

within the Department of Health and Human Services, along with the Food and Drug Administration, imposed unclear, contradictory, and eleventh-hour standards on VaxGen. (Rhodes, 2007)²¹ In December, 2006 the government canceled the VaxGen contract entirely, with no product of any sort or show for its investment. The whole BioShield program has been criticized as lacking in strategic direction and buffeted by intense lobbying by biotech firms. (Anon., 2007; Trull et al., 2007; Lipton, 2006)

However, as the troubles with BioShield mounted, Congress did take note. Hearings were held, bills introduced, debate facilitated. In April 2007, Congress created the Biomedical Advanced Research and Development Authority (BARDA), which has been given a relatively free hand to experiment with policy design. This move is very desirable, given the numerous and subtle challenges involved in running a government program to discover and produce quantities of bioterrorism-related vaccines. (Chapter 15) They range from the simple design of incentives to the management of liability concerns to the protection of programs against predictable efforts (both by the government and by research entities) against tactics to abuse and even defraud.

We have already noted that the projected outlays of \$1.2 billion by the Domestic Nuclear Detection Office for ASP cargo screening equipment look ill-advised. Most disconcerting of all, the whole Science and Technology Directorate of the DHS, which managed most of the R&D effort, was, overall, poorly managed from its inception. A congressional report in 2007 characterized the directorate as “a rudderless ship without a clear way to get back on course,” criticized its lack of clear research goals, absence of detailed budget information, mystifying accounting conventions,” and its inability to spend prior-year appropriations. (AAAS, 2007) A new director, Rear Admiral Jay Cohen, who has had long experience as head of the Office of Naval Research, took office as Under Secretary for Science and Technology soon thereafter and moved quickly to reorganize the staff and refocus the effort. (Magnuson, 2007)

The DHS R&D effort is closely related to the Department’s procurement process, which has also been very troubled. Despite some bright spots, such as initially bringing in veteran Defense Department procurement specialists to establish procedures, and relying heavily on a special acquisition authority known as “other transactions” to carry out prototype and other non-standard projects (GAO, 2005) procurement has been widely criticized. “Hordes of critics, including former DHS executives, watchdog groups, the Government Accountability . . . and Congressmen by the dozens have excoriated the

department's procurement record." (Gregory, 2006)²² Not only did it fail to perform but it permitted waste on a large scale, as was evident in the aftermath of Katrina. Prof. Steven Kelman of Harvard's Kennedy School of Government, a procurement expert, and former head of the Office of Federal Procurement Policy, attributed the problems primarily to lack of adequate manpower relative to the rapidly expanding workload (Gregory 2006) – a problem we noted above in conjunction with implementation of C-TPAT. The DHS, like much of the federal government, has also been losing top managers to the private sector (and to retirement) at an alarming rate. (Hsu, 2007)

8.5 Developing Institutional Capacity

Money is versatile, powerful, and, assuming deficit financing, relatively easy to come by. It can even be used to improve institutional capacity, e.g., by buying more and training better front-line freight inspectors, or by purchasing interoperable communications equipment, or by setting up a whole new office dedicated, say, to domestic nuclear detection. But in the final analysis, money cannot do much to improve institutional capacity, especially within government bureaucracies. The incentives and constraints that limit performance apply whether the bureaucracies are well- or poorly-funded. Public sector bureaucracies normally attempt to protect their autonomy, augment their budgets, avoid conflict, deflect accountability, maintain discretionary resources, and go by the book.

(Wilson, 1989) They generally are slow to innovate, reluctant to collaborate, and cautious about new missions that could interfere with their old missions.

Sometimes there are exceptions, e.g., when there is a crisis accompanied by political expectations for bold new action, or when a new leader is installed who wants to make a reputation for himself or herself. But in general, the American tradition in public administration is to hamstring bureaucracy in the hopes of keeping it limited and non-abusive, even if doing so might also mean keeping it relatively ineffective and inefficient.

That said, the need to deal with the threat of terrorism and WMD has given rise to a universal consensus behind new and improved institutional capacity. True, there has been conflict over the details, sometimes bitter conflict, e.g., over whether to create a new homeland security department. But on the desirability of capacity-building *per se*, agreement prevails. Capacity-building has appeared in four basic forms:

- Creating new organizations more or less *de novo*.
- Reforming or re-engineering existing organizations.
- Reorganizing existing organizations.
- Improving interorganizational cooperation.

Of these four types of capacity improvement, the first is much less problematic than the others, and I will not discuss it. The other three are immensely challenging, and the landscape of public administration is probably littered with more failures than successes – and with an even greater number of specimens for which capacity improvement has not even been tried. Before turning to a discussion of these three, though, I shall say a word about the meaning of “success” and “failure.”

“Success” and “failure.” It is, in general, hard for the public to perceive the true results of efforts at institutional capacity-building, because the details of implementation are largely hidden; and those that come to light probably represent either unusual successes or unusual failures. Moreover, it is ambiguous what the appropriate standard ought to be by which to evaluate success or failure. For instance, DHS is widely criticized as being a low-performing agency. (Kettl, 2007) But, as is always true of policy and management, the critical question is, Compared to what? In this case, is it plausible that the reorganization into a single umbrella department of 22 formerly separate agencies has improved their performance relative to what it would have been had the present trends, which included more voluntary cooperation, been allowed to continue, or to have continued with some boost delivered by less drastic means? The answer is more likely yes than no, especially if we consider the long run.

Many critics of DHS hold it to a standard derived from a sense of what, ideally, we would like it to be able to do. That is also reasonable, especially when there is consensus on appropriate performance standards, neither impossibly high nor unjustifiably low. For instance, the failure of FEMA, and indirectly of DHS, to respond effectively to Hurricane Katrina was consensually recognized as such, even by the Bush White House.²³

One must also make allowances for trial-and-error learning. Building institutional capacity for dealing with WMD is exceedingly complex. Mistakes will be made, even very costly mistakes. How many such mistakes, and which ones, should be written off as appropriate trial-and-error learning, and how many, and which ones, debited to the poor-performance account of our institutions or our leaders? Furthermore, how much delay is optimal in sorting out legitimate disagreements over the many technical and value-laden issues that beset the process? And how much represents an indictment of “sluggish bureaucracy” or “foot-dragging, turf-protecting bureaucrats?”²⁴

8.5.1 Reform/reengineer existing organizations

Government agencies are notoriously difficult to reform or reengineer. Some of the main barriers are statutes that constrain managerial discretion over organizational structure and, more importantly, funding streams for identifiable programs or organizational units. Another barrier is civil service definition of job descriptions and the protection of employee tenure; and in some cases civil service protection is backed also by collective bargaining agreements. In the case of our national security and law enforcement agencies, professional pride in mission and historical expertise can also stand in the way (Zegart 1999), although these can also be a source of innovation and change.

Among all the counter-measures we can take vis a vis WMD, improving our intelligence capability is probably the most cost-effective. This comes about partly because the damage wrought by a successful WMD attack would be shockingly great, even if optimal response and recovery could be assumed; hence, the value of preventing it – for which intelligence is central – is very high. Secondly, because prevention-oriented intelligence could protect anywhere from dozens to hundreds of potential targets it is, in effect, buying security at wholesale rather than retail prices. Nonetheless, upgrading our intelligence capabilities, both foreign and domestic, has proven exceedingly difficult.

UCLA political scientist Amy Zegart has estimated that 84% of 340 intelligence recommendations made by twelve different study groups between 1991 and 2001 about dealing with the threat of terrorism reappeared in the post-September 11 analyses by the September 11 Commission and/or a parallel Congressional Joint Inquiry into the attacks. (Zegart 2007) Her inference is that the terrorist threat was well understood but that the Intelligence Community (IC) failed to rise to the challenge. Zegart's explanation as to why this occurred emphasizes the fragmentation within the IC (many separate agencies with separate power bases and, within the CIA, internal "stovepipes"); career success dependent on the number of "products" produced (spies recruited, items in the President's Daily Brief, etc.) rather than on their quality; and a culture shaped by the Cold War which, among other things, inhibited information sharing both horizontally (across agencies and stovepipes) and vertically (between collectors and analysts).²⁵ Of course these and related problems can, in theory, be somewhat offset by determined and creative leadership. But there is a history of Presidential and Congressional indifference to intelligence reform, an indifference rooted in rational political incentives to attend to more visible and less difficult issues. (Zegart 2007)

The FBI, which is the closest thing we have to a domestic intelligence agency, is an even more troubling story. It has long been understood that all the

incentives within the FBI lead the agency to downplay primary prevention (before the onset of trouble) via intelligence in favor of secondary prevention (preventing recurrence) via criminal enforcement and incapacitation. Apprehending malefactors and locking them up is how FBI agents traditionally earn prestige and advancement, not disrupting terrorist networks or acts. (9/11 Commission, 2004; Hitz and Weiss 2004)

The country has faced a choice between creating an effective domestic intelligence and counter-terrorism capacity within the FBI or setting up an entirely new agency analogous to Britain's MI5, which has as its only mission to gather intelligence and cannot bring cases against individuals. So far, we have taken the first route. Whether that choice has been effective is debated. Arguably, if we were writing on a clean slate, we would have gone the second route. But, given that the FBI exists and its supporters bitterly oppose a new agency and would probably have to compete with it for status and budget, and that such rivalry could undermine cooperation between the FBI and such a new agency, the choice is not so clear.²⁶ Much depends on how well the FBI is implementing the internal changes required to make it into an effective domestic intelligence and counter-terrorism agency.

FBI Director Robert Mueller, who assumed his post a week before the World Trade Center was destroyed, seems to have aggressively pursued an agenda of what the FBI itself calls “agency transformation.” (FBI, 2004, 2006; Anon., 2006)²⁷ Five years after September 11, the FBI publicized a lengthy list of actions it had taken along these lines, including the creation of a National Security Branch in September 2005 and a Weapons of Mass Destruction Directorate in July 2006. During this time it also increased, among other things, its multi-agency Joint Terrorism Task Forces from 35 to 101; increased its agents and police officers on these bodies from about 1,000 to 4,000, and increased its “on-board linguists” from 784 on September 11 to 1430, and its Arabic linguists from 70 to 269. (FBI, 2006)

Congressional testimony around the same time by Richard Thornburgh, a close observer of the FBI and US Attorney General, praised the Bureau’s transformational efforts and accomplishments. Thornburgh is chairman of the FBI Transformation Panel of the National Academy of Public Administration, which had been consulting with the FBI on a wide range of managerial and programmatic issues. Thornburgh listed a number of improvements to the agency’s general management capacity which had apparently been much needed, in areas like budgeting, human resources, and strategic planning. He also pointed to two new career paths within the FBI, probably the most crucial change the

Bureau could be undertaking: for Special Agents in intelligence, and professional staff in Information Technology. (Thornburgh 2006)²⁸

As noted earlier, there is often a large gap between the formal actions of an agency, such as creating a new career track, and their real significance in implementation. Judge Richard A. Posner, an incisive social observer who has studied intelligence failures, pronounces the transformation effort a failure and renews his call for a separate domestic security agency. (Posner, 2006) Reporting on a February 2006 conference of top FBI officers from across the nation, the *New York Times* wrote: "...F.B.I. culture still respects door-kicking investigators more than deskbound analysts sifting through tidbits of data." And "knowledgeable employees" said that "Muslim agents number no more than a dozen of the bureau's 12,664 agents. (Shane and Bergman, 2006) The most indicative commentary comes from the May 2006 testimony of John Gannon, "a respected senior intelligence official who had spent 24 years working with the FBI in various positions" ranging from the CIA to House homeland security committee staff director, who said "I have changed my mind [about the FBI's potential for developing a domestic intelligence capability]. I now doubt that the FBI, on its present course, can get there from here.'" (Zegart, 2007)

So far we have been discussing the dynamics of bureaucratic behavior as barriers to adaptation. We should not overlook the barriers to reform and reengineering created by government-wide rules intended to prevent waste, fraud, and abuse, but that so often undermine many agency managers' and operatives' desires to improve performance. Air marshals anonymously take flights so as to be available in the event of a terrorist attack. But the rules are the rules:

Agents are required to check in at airport ticket counters, and in most cases display oversized credentials. Until recently, a jacket-and-tie dress code was mandated on all flights, even those filled with tourists headed for Disney World. They also were instructed to stay in designated hotels, where they had to display their marshal credentials to secure a discounted rate. (Meckler and Carey, 2007)

8.5.2 Reorganizing

By any standard, there has been a lot of reorganizing. The Department of Homeland Security brought under one hierarchical roof – on paper, at least – 22 separate organizations. The Intelligence Community was given a controversial hierarchical superior, the Director of National Intelligence (DNI) – though the extent of his authority is an open question. The National Counterterrorism Center

(NCTC) is comprised of elements of the DHS, the FBI's Counterterrorism Division, the Counterterrorist Center based at the CIA, the Department of Defense, and other agencies. Customs and Border Protection (CBP) was created by merging the Customs Bureau, the Border Patrol, and the inspectional functions of the Immigration and Naturalization Service (INS) and the Agriculture and Plant Health Inspection Service (APHIS).

In the public sector, reorganizations stem from many motives, ranging from the elimination of (supposedly) costly redundancy to the political domestication of a distrusted agency. The two most visible reorganizations in the federal government's response to terrorism have been the DHS and the DNI. These have been prompted by the desire to reduce policy and operational fragmentation, that is, by a desire to increase effectiveness and efficiency. The prevailing theory has been that a common superior could improve resource allocation, planning, and operational coordination. In addition, the lines of accountability to the White House and to Congress would become clearer and more effective. Such a theory motivated the largely successful reorganization of the military commands and the Joint Chiefs of Staff by the Goldwater-Nichols Act of 1986. (Locher, 2002)²⁹ There are severe limitations to centralization and hierarchy, however, and it is not clear just how applicable it is to a world in which situational complexity and volatility are dominant facts of life. This is one reason

– among the many powerful political reasons that constrain and distort such matters (Zegart 1999) – that the reorganization of the Intelligence Community under a DNI is itself very limited.

Assuming reorganization is necessary, it would be desirable for the reorganization to be implemented expeditiously and effectively. This requires leadership to mobilize needed resources and focus energy and attention. No such leadership aided at the birth of the DHS. Indeed, almost the opposite seems to have occurred. (Brzezinski, 2005) Knowledgeable informants have also been severely critical of DHS's failure from the first to think strategically about appropriate mission priorities (number one, for them: securing ordinary infrastructure that could be turned into weapons) or resource priorities (number one: mobilizing the business sector). (Benjamin and Simon, 2005)

Why this process was so apparently sluggish and unfocused is unclear. True, President Bush had opposed the creation of a single homeland security department for several years. But once it was official, it could only make sense to move rapidly and efficiently. Instead, the President appointed Tom Ridge, a feckless leader (Benjamin and Simon 2005), as its first Secretary, and then tried to install Bernard Kerik as his successor. Kerik had no federal experience, a history of corruption, a reputation as a bullying leader (Blumenthal 2004), and a mixed

track record of training a police force in Iraq. (Bumiller, 2004) The process also appears to have allowed the counter-terrorism mission to have degraded the capabilities of at least one important agency. The Federal Emergency Management Agency (FEMA), which had briefly flourished during the Clinton presidency, spiraled downward badly during the Bush presidency and its absorption by DHS. (Brinkley, 2006; Beers and Clarke, 2006; Grunwald and Glasser, 2005)

8.5.3 Interagency collaboration

“Interagency collaboration” is typically a challenge for agencies, principally because agencies reflect the career and professional interests of those who work for them, and those interests are typically best served by the autonomy of their agencies against outside threats to jurisdiction, claims to expertise, and promotion ladders. The interests of legislative overseers are also typically served by the autonomy of “their” agencies, since the power of oversight committees depends on their agencies’ autonomy. Rational strategic behavior aside, agencies also tend to develop a boundaries-based, tribal culture in which loyalty inward is nurtured and loyalty outward is viewed with suspicion. (Bardach, 1998; Wilson, 1989)

The problem, of course, is that the modern world changes too rapidly for jurisdictions and habits to keep up. Reorganizations are slow, wearing, and bring

mismatches of their own. Informal collaboration is often the only hope of matching problems and solutions. Nowhere is this truer than in the world of counter-terrorism. And because the concerned agencies are staffed and led by large numbers of public-spirited people, the unnaturalness of collaboration, and its many pitfalls and technical challenges, may be overcome to some degree. Studies of different agencies learning to work together in high-risk families, habitat protection, environmental enforcement and other domestic contexts shows that, despite difficulties, productive collaboration does sometimes occur. (Bardach, 2008, 1998) In the area of disaster response, a template for multi-agency and multi-jurisdictional cooperation has been available for over thirty years now in the form of the Incident Command System. It has generally worked well and is prescribed by the DHS National Response Plan, though some scholars doubt whether it can work effectively in catastrophes or even in certain types of disasters. (Rubin and Harrald, 2006; Buck et al., 2006)³⁰

Collaboration problems are ubiquitous in Homeland Security. Local hospitals and clinics need to collaborate on planning for mass casualties; the CBP, US and foreign ports, the Coast Guard, the DND, shippers, customs brokers, equipment vendors, and many other parties must coordinate to manage supply chain security; federal, state, and local agencies need to coordinate in the event of a catastrophe with significant jurisdictional spillovers; local police departments

share intelligence with one another and with the FBI (which, however, is said rarely to reciprocate); more centralized coordination of the Intelligence Community had been recommended by study commissions and other observers for many years, though it was successful only in the political environment following September 11. The Office of the Assistant Secretary for Preparedness and Response, within the Department of Health and Human Services, and the Food and Drug Administration have tried, with mixed success to work out approval standards for BioShield products. (Rhodes 2007)

Interorganizational cooperation takes many forms. Sometimes it is institutionalized as a formal, ongoing program like the Container Security Initiative (CSI), which aims to inspect and clear containers before they are shipped from foreign shores. Others, such as the DHS's SAFECOM (sorting out interoperable communications technology), involve joint policy planning but not much in the way of operational coordination. Still others, organized around emergency events, combine pre-event planning and post-event response coordination.

It is worthwhile differentiating two rather different collaborative contexts, however. One involves agencies that are sufficiently different so that competition is not a zero-sum game that potentially threatens the existence of either partner.

An example would be a local police department, radiological specialists from the US Department of Energy, and the state highway patrol engaged in a search for a threatened “dirty bomb.” Or we might have CBP officials, port security staff, shippers representatives, and the Coast Guard working out a plan to prevent a ship from docking until its inspection history can be validated.³¹ Here agencies are merely wary and defensive of one another, each fearing, let us say, that collaboration might oblige them to sacrifice resources to the common effort or alter their mission priorities. While individuals – and agencies – might jockey for primacy, maneuver to offload work onto one another, and make life difficult for one another by proposing incompatible standards and protocols. Nevertheless, in the end, they will work things out.

The situation is more threatening where agencies are rivals that compete head-to-head for the same spotlight or funds or other resources, such as information or informants or control over cases. Here, one agency’s success just might come at the expense of the other. Almost certainly some aspect of this rivalry has been slowing down the recognized need for “the major national security institutions ... to create a ‘trusted information network.’” (Public Discourse Project, 2005a) Not only are the agencies on the defensive but they may be on the offensive as well. In this more threatening context, we have the examples of the Army claiming the right to fly its own aircraft in certain

situations and the Air Force contesting that claim (Wilson 1989); the FBI investigating the CIA in the aftermath of the Aldrich Ames betrayal; the CIA refusing to advise the FBI of the magnitude of its losses in the Ames case or give the FBI access to its files (Mahle 2004); and the CIA and the FBI trading charges in *Time* and *Newsweek* that it was the other agency's responsibility for having lost the trail of two of the September 11 attackers on their way to the US. (Tenet, 2007)³²

This last set-to between agencies that ought to cooperate but historically have not done so marks a less obvious set of interagency problems as well. In his recent memoir, CIA Director George Tenet provides a detailed history of how the FBI and the CIA actually cooperated willingly and competently on the Malaysian suspects, over a period of many months. (Tenet, 2007) Agencies are composed of many units, differentiated as well as integrated, and one of the most important bases of differentiation is formal hierarchical authority. Even if the senior officials have good working relationships across unit boundaries at the same hierarchical level, the good will may not flow down the hierarchy very far within each of the units taken separately. And *vice versa*: if line-level staff of different agencies, say, have informally developed a team approach to a shared problem, they might discover that their supervisors are not pleased. Interests, values, and situational understandings can differ greatly from one stratum of the hierarchy to another. In

the case of the Malaysian suspects, the agencies' operatives were working together effectively, with the indirect blessings of the agencies' Directors, but their press offices and probably other personnel too acted out old scripts.

There are no simple answers to how to get rival agencies, as opposed to merely defensive agencies, to work well together. High stakes for the public and for agency employees probably help a lot, though they are no guarantee of success. Even in wartime, the US armed services have not been able to overcome rivalries in the past, even when many lives and great strategic objectives were at stake. (Locher, 2002) A shared culture of professionalism and intense commitment to a mission almost certainly helps. The National Counterterrorism Center (NCTC) brings analysts together from different agencies to draft collective reports. The Center also provides on-line intelligence syntheses to a variety of users. It is "widely considered to be one of the most successful improvements in US intelligence." (Zegart, 2007) Nevertheless, interagency barriers decrease its effectiveness and efficiency. Because the analysts have different security clearances, they still see different information; the information is stored on nearly 30 separate, and incompatible, networks, which require access to six different computers stored under analysts' desks. ("Pizza boxes" is the wry epithet in common use.) And "officials still resist sharing information with colleagues assigned from other agencies even when the rules allow it." (Zegart, 2007)

Two other helpful ingredients are committed leadership and an effort to sit down and hammer out an explicit understanding about the division of labor and responsibilities. (Goldsmith and Eggers, 2004; Bardach, 1998) Such understandings are inevitably incomplete and are likely to dissolve once the original actors depart . But given time, some progress is possible. In rare cases, a common superior can knock heads together and assert a resolution. It took decades to resolve a standoff between the fire and police departments in New York City that persisted even after their egregious failures of cooperation on September 11. (Confessore, 2005)

In this connection it is worth noting the seemingly successful effort of DNI Mike McConnell and a number of other high-ranking officials in the Intelligence Community to create a joint-duty program. Modeled on what was done in the military by Goldwater-Nichols, it requires that senior management appointees in the IC have served 1-3 years outside their home agency. It also includes an educational component. The rationale is to create in the IC “a broad, enterprise-wide focus, ...about developing leaders with the ability to integrate all of the IC’s assets to accomplish [its] mission.” (ODNI, 2007) Although a similar program had begun in the late 1990s under George Tenet, it had run into a buzz-saw of

agency opposition. The current effort has powerful and extensive interagency support and already counts some 1500 participants.³³

8.6 Learning

In order to adapt to the WMD challenge, policy-makers and implementers must contrive to learn as they go along. They must learn about the very matters discussed in this chapter so far: about the nature and magnitude of the challenge, the level of resources that need to be marshaled, how to expend them wisely, how best to stimulate and partner with the private sector, and how to build institutional capacity. Furthermore, they must create the capacity for learning per se. This means building institutions that specialize in learning and disseminating what is learned. It also means creating a culture that respects facts, analysis, and rational argument.

Political elites tend to be short on such virtues. Nevertheless, policy learning does occur, albeit slowly, unevenly, and sometimes at high cost. Homeland security seems to me to fit this general pattern. I shall organize the comments that follow according to the experiential sources of learning: Events, general experience with policies and institutions, “best practices,” simulations, and controlled evaluations.

8.6.1 Learning From Events

The experts and commentators talk and write, but is anybody listening? No organizations, and especially no public organizations and their elected leaders, are very good at learning from events. (Levinthal and March, 1993; Lynn, 1997) A poor federal response to Hurricane Andrew in 1992 led to a successful upgrading of FEMA during the Clinton years, but the subsequent Bush administration permitted the agency's capacity to degrade substantially. According to a team of engineering faculty based at UC Berkeley, the flood protection system being rebuilt in New Orleans following Hurricane Katrina "has not been significantly improved...Filling levees with the shells that washed out of them is like giving a Band-Aid to a patient in need of a triple bypass." (Spotswood, 2006) A comprehensive analysis of the anthrax attacks and subsequent scare of October 2001 refers to "an unacceptable level of fragility in systems now properly recognized as vital to national defense" and continues, "Most of the vulnerabilities in the medical and public health systems revealed by the response remain unaddressed." (Gursky et al., 2003) A history of urban terror attacks in Jerusalem, Israel, since the 1990s should have taught the Israelis the importance of an organized response system such as an ICS. It seems to have had little or no effect, however, as the response to terror events even in 2002 was anarchic, with fire department vehicles blocking access roads for ambulances to the disaster scene while police were reporting these roads open. (Perliger, 2005) The US

Army, following the trauma of Vietnam, “threw away virtually everything it had learned there, slowly and painfully, about how to wage a counterinsurgency campaign.” When it went to war in Iraq in 2003, its “core document,” the 1976 edition of its field manual, “did not mention counterinsurgency.” (Ricks, 2006) The very same sort of organizational flaws in NASA and its contractor network that led to the demise of the Space Shuttle Columbia in 2003 had been diagnosed following the Challenger disaster 17 years earlier. (Mahler, 2008) Impeding successful organizational adaptation, the external and internal pressures on NASA to launch flights were also aggravated by internal politics, organizational processes, and poor risk management practices.

Such failures aside, events do provide opportunities for learning. Fortunately, these opportunities are rare. The US and the world have never had an opportunity to learn from a successful WMD event in peacetime. The closest we have come were the 1995 nerve gas attack by a Japanese religious cult on passengers in the Tokyo subway, in which 12 commuters were killed, 54 seriously injured, and another 1,000 or so affected, and the anthrax attacks in the US in October 2001.³⁴ However, learning can be based on analogous situations, such as very large-scale natural disasters, and on “near-events” such as the attempt to destroy the World Trade Center in 1993 and the failed efforts by jihadist organizations to shoot down civilian aircraft with shoulder-fired missiles.

We have had plenty of such situations. Leaving aside whether learning gets translated into organizational action, it is safe to say that important people, including elected officials, senior managers, thoughtful professionals, and many informed laypersons, have learned from these situations, often a great deal. What is learned falls into two general categories: this threat/vulnerability/damage-function is worse than we thought it was; and, this prevention/preparedness/response system is less coherent/effective/responsive than we expected it to be.

Since the Progressive era, when the nation discovered the hazards of meat and patent medicines, the list of real or supposed environmental threats has only grown. This development is a function both of an increasing sense of (assumedly costless) entitlement to safety and a greater scientific understanding of the pathways along which danger travels. Periodic outbreaks of illness, deaths in mine disasters, casualties of drug side-effects, lead paint, oil spills, train wrecks, black lung disease, and so on accentuate the general trend and frequently lead to new protective legislation.³⁵ The same pattern holds with respect to natural disasters. (Birkland, 2006) Since Katrina, for instance, DHS and FEMA have been giving much more attention to all-hazards preparedness, rather than more narrowly to terrorism. (Skinner, 2006)³⁶ The post-September 11 reaction

sketched above in Section 8.1 suggests that the same can be said about terrorist events. Similarly, within weeks of the 2004 railway bombings in Madrid, Spain, the US Congress appropriated an additional \$100 million in railway security grants for FY 2005. (Stowsky, 2006)

But if events can sometimes focus attention on inadequacies of problem-recognition and/or response, they do not usually teach much about the nature of cost-effective remedies. Learning what not to do rarely implies learning what to do. (Birkland, 2006) An excellent case in point is the finding of the 9/11 Commission that the FBI and the CIA had failed to “connect the dots” so as to see the emerging threat and preempt it. Sufficient data existed, said the Commission, but it was not transmitted or, if transmitted, not acted upon. Al Qaeda was more dangerous by far than we had recognized, and our capacity for prevention far worse. With regard to learning, so far so good. The Commission went a step further, however, and recommended solutions to the problem, including the creation of a DNI with enough authority to re-engineer the way the disparate members of the Intelligence Community shared information and formed operational plans. The recommendation was, in part at least, adopted some months later. Whether this will prove to have been a wise measure remains to be seen.

Although events do not teach what to do, they do open a “policy window” (Kingdon, 1995) for a discussion of ideas already current among elites who have been attending to the policy area for some time and have built up a store of evaluations and reasoned speculation for some time. (9/11 Commission, 2004; Haveman et al. 2005). Nearly all of the recommendations of the 9/11 Commission, for instance, had been known for years. The existence of such policy elites, and their file cabinets full of proposals and arguments, increases the odds that reasonable ideas will eventually be implemented. They are far from a guarantee, however. If it is too economically or politically costly for policy-makers to act, or if there is dissensus among elites on which policies should be adopted, as often happens when interagency collaboration is involved or reform of the intelligence agencies (Zegart, 2007), the policy window may close with nothing being done – until perhaps there is another event that focus attention and re-opens the policy window. (May, 1992; Birkland, 2006)

8.6.2 Direct Experience With Policies and Institutions

The Congress learned from years of experience that it had to find ways to avoid turning the state and local grants into pork barrel programs, though it has only partially succeeded. The DHS has slowly been learning how to introduce more technical rationality into the distribution formula, via risk assessment (and, to a lesser degree, the assessment of local implementation effectiveness. (GAO,

2007b) Given the disparate origins of the 22 agencies composing the DHS, it is not surprising that the trial-and-error efforts to organize and reorganize have been continuous. The largest appears to have occurred in July 2005, five months after Michael Chertoff took over from the first DHS Secretary, Tom Ridge: the major divisions of the department were dissolved and then reassembled.

As I noted above, after some early, and massive, disappointments with BioShield, the Congress in April 2007 created a new implementation structure, BARDA, which seems to promise a much more flexible and creative approach.

It is through experience, and the sophistication of understanding about governmental institutions, that policy-makers detect inadequacies and take measures to correct them. Examples such as those above could be multiplied almost indefinitely. The important questions, though, are (1) how well and how fast governmental actors recognize their own mistakes and begin to correct them and (2) to what extent the “solution” actually improves on the problem. And in the present context, how does learning from this sort of experience in the WMD area compare with such policy and implementation learning more generally?

To answer these questions in a systematic way is well beyond the scope of this chapter. In the “Summing up” section below, though, I attempt some speculation.

8.6.3 Best practices

In a federal system, different jurisdictions have opportunities to learn from one another. States, Justice Louis D. Brandeis famously said, are “the laboratories of democracy,” and there is some evidence that states do look to each other as sources of ideas. Federal agencies like the Environmental Protection Agency (EPA) and the Occupational Safety and Health Administration (OSHA) follow a strategy of devolving programmatic functions to the states, rendering technical assistance and then reporting regionally or nationally on “what seems to be working.” Analogously, state agencies often do the same for cities and counties. The particular vehicles for disseminating ideas are varied, ranging from workshops, conferences, and professional association meetings to web sites, newsletters and journals.

State and local governments play a central role in preparing for and responding to disasters. The seeds of the current Incident Command System were sown by the highly disorganized response to a series of forest fires in Southern California in the early 1970s. They were nourished subsequently by professional fire-fighting networks in California and around the country and in particular by the US Forest Service for state forest fire fighting agencies, and by the US Fire Academy for urban fire departments and volunteer fire companies. (Buck et al.,

2006) The Incident Command System is often a very effective response (Bigley and Roberts, 2001) and is now enshrined as the technical basis for the National Response Plan, which is what would be invoked in the event of a successful WMD attack in which the federal government became involved (which would almost surely be the case). Here, surely, is a case of the dissemination of “best practice,” and of societal learning, to be proud of – provided the ICS actually works, which, as I remarked above, is somewhat in dispute.

8.6.4 Simulations

Scores of simulations, drills, and exercises take place every year at all levels of government and in the private sector. (Phillips, 2006; Brzezinski, 2005) The three main functions of these are to stimulate preparedness planning, to practice response routines in the event of an attack, and, in after-action reviews, to diagnose weak points in preparedness and execution. This last function is probably the most important when it comes to catastrophes. No matter what organizational arrangements are planned for the response phase, that is, an Incident Command System or something else, a great deal of preparatory training is required. It just won't do to have the managers from participating agencies exchanging their business cards with fires (or germs or radiation) swirling around them. Unfortunately, disaster-scale simulations are expensive and hard to

organize. Hence, simulations are relatively infrequent – and catastrophe-scale simulations even less so. (McConnell and Drennan, 2006)

The best-known of the catastrophe-scale simulations is the Congressionally-mandated TOPOFF exercises (the contraction denotes participation by “top officials”), the first four of which took place between 2000 and 2007. The first enacted simultaneous events in Denver (an attack of plague bacteria); Portsmouth, New Hampshire (chemical weapons); and the Washington DC area (a radiological event). (Inglesby et al., 2001) The exercises were supposed to take place “without-notice,” but in fact were widely known beforehand. Realism was compromised in other important ways as well: In the Denver case, the Colorado governor was not involved nor was the role simulated nor were other political figures involved; a non-political Emergency Epidemic Response Committee of medical experts (EERC) was improvised to handle the crisis on its own. Many of the unfolding elements were hypothetical such as masses of patients showing up at hospitals to demand antibiotics, and these events were “injected” by the TOPOFF managers into the information streams of the participants.

Despite these limitations, the first TOPOFF exercise was highly instructive, identifying problems that would otherwise have gone undiagnosed.

The EERC and a larger committee of community-wide decision-makers wasted endless time in conference calls, some involving 50-100 persons, whose roles, authorities, and even identities were unclear. (Inglesby et al., 2001) Public health professionals proved unfamiliar with the jargon and acronyms used in the emergency management community, such as the JIC, the JOC, and the DMORTs.³⁷ Mock antibiotics delivered to the airport were being unbundled by a single individual who “‘had to count individual pills and put them into plastic baggies.’ Before she could even begin, there was a six-hour delay during which (hypothetical) traffic was negotiated ‘in order to get the plastic baggies from Safeway.’” (Inglesby et al., 2001)³⁸

Whether such learning counts for anything, of course, depends on the nature and quality of the follow-up. A 2004 simulation of a Category 3 hurricane hitting New Orleans, complete with storm surge overtopping the levees, did illuminate some lessons “‘later applied with successful results,” “but as a whole, the system seemed unready despite the rehearsal.” (Phillips 2006) FEMA canceled much of the follow-up work citing lack of funds, including a projected study of how to find long-term shelter for evacuees housed at the Superdome.

Overall, however, the country has been working successfully at improving the design of simulations and systematizing the process for learning from them.

RAND's online Public Health Preparedness Database, which includes nearly forty simulations of terrorist attacks and infectious disease outbreaks. And a National Memorial Institute for the Prevention of Terrorism, funded by the DHS, hosts a Lessons Learned Information Sharing web site that gives registered users access to after-action reports on various exercises. (Phillips, 2006)

8.6.5 Evaluations

Evaluations come on a continuum, from those that, in a methodological sense, are highly controlled to those that take advantage of what appears to be “common sense.”

The better controlled. In a domain as vast as domestic security, there are many opportunities for controlled evaluations. Pieces of hardware such as the spectroscopic portal monitors (ASPs) mentioned above are easy to test rigorously. They are less easily tested *in situ*, but it is still good practice to pilot-test hardware in field situations before full scale deployment. As the ASP case suggests, however, deployment sometimes ignores test results.

Organizational practices, such as how to conduct and make use of simulations, or how to run an effective public communications operation in times

of emergency, or how to ensure that pharmaceutical stockpiles are expeditiously accessed and distributed, are harder to test. Very occasionally, managers make use of “planned variation” in which individual units evaluate novel practices in order to find out “what works” so that best practices can be disseminated. An example would be having field offices of a county welfare agency try different case management procedures and comparing results.³⁹ More common – though still a relative rarity given its potential value – is the communication across field offices of seemingly good ideas that have spontaneously emerged at one or more sites. This sort of process would be ideally suited to the FBI, say, although I do not know whether it actually occurs. To facilitate such intra-organizational learning almost certainly depends on top leadership seeing to it that field-office directors do not regard such a process as infringing on their autonomy or a way to make invidious comparisons.

The less well controlled. At the opposite end of the continuum we have evaluations of the sort done by the GAO, which typically involve linking performance deficits in some federal agency (or ensemble of agencies) to common-sensically derived suppositions about one or more deficiencies in the agency’s (or agencies’) structure or set of practices. The GAO has paid extensive attention to counter-terrorism, WMD, and the relevant agencies.⁴⁰

Congressional oversight committees, of course, are active in this area – sometimes too much so, as they are numerous and consume many hours of top executives’ time preparing and giving testimony.⁴¹ Because of the political sensitivity of the issues, along with security concerns, a fair amount of evaluating, analyzing, and reviewing, is turned over to specially appointed commissions, such as the National Commission on Terrorist Attacks Upon the United States (“the September 11 Commission”). The US also hosts many public policy think tanks whose affiliated analysts and researchers have been scrutinizing homeland security issues since September 11 and in many cases before. Many of their products have been referenced in this chapter.

These are capabilities housed essentially outside of executive branch agencies. It would make sense to have policy analytic and evaluation capabilities at work within the agencies as well, analogous to the “policy shops” in the Department of Defense and in certain domestically oriented agencies like the Department of Health and Human Services. Unfortunately, the Department of Homeland Security did not have such a policy shop until April 2007, that is, for the first four years of its existence.

8.6.7 Summing Up.

Unfortunately, the social science literature on how governments, or policy-making elites, learn or fail to learn is slim and is lacking in explanatory and predictive power. Most of the literature considers the learning process through lenses appropriate for individual behavior, particularly information processing. It tends to downplay the existence and functioning of very complex processes of inter-individual and inter-institutional connectivity or lack thereof; self-interestedly motivated indifference or distortion; and the uses of what might be called “pseudo-information” in symbol manipulation. Yet, I would like to use at least a rudimentary theoretical framework in order to assess whether governmental learning in the area of WMD threat management is better or worse than what we see on average. My simple framework begins with the supply and demand for “problem-solving rationality,” particularly the sort of rationality that is focused on realistic problem recognition and on critical evaluation of purported solutions. In this context, “solutions” includes the whole array of social practices we call “programs” and “policies” and “institutional procedures,” and so on.

First consider supply. American government is blessed with large numbers of professionals who are paid to give (or take) what they deem to be rational and disinterested policy advice. They mostly occupy staff positions in both the legislative and executive branches. In addition, many of the relevant action agencies of government are headed and/or staffed by professionals who are

at least intendedly rational in their own fields of expertise, e.g., fire chiefs, public health directors, emergency management experts. Many of these individuals, and the organizational units that employ them, produce reasoned and reasonable advice. Some, indeed, are extremely talented and dedicated. Furthermore, the in-house pools of such advice are augmented by an army of contract consultants to government, just as is found in the private sector, and analysts working in think tanks. Is there reason to think that the pool of rational problem-solvers is smaller or larger in the WMD domain than in other policy domains? That it is more talented and dedicated than average or less so?

On the one hand, the subject matter probably attracts individuals who are somewhat above average in problem-solving talent and dedication than government in general, much as one expects to find in the ranks of military officers. The problems are intellectually and morally challenging, and come with an aura that attaches to issues of collective fate. On the other hand, outside the Intelligence Community, and possibly the GAO, the relevant institutions are for the most part nothing special when considered as places to make a government career, e.g., a local public health department or a state emergency services agency or a federal procurement official concerned with contracts for radiation detectors.

They are not bad places at all, but neither do they radiate glory. In the think-tank and consultancy sectors, the quality of talent is high, as it is in the

WMD domain as well. The net result is that, when it comes to the supply of good policy-analytic thinking, the WMD domain is probably as well off as we find in other policy domains and perhaps a little better.

Turning to the demand side, policy rationality is not much wanted. The protection of private interest – commercial, financial, bureaucratic, political – greatly dominates the disinterestedly rational pursuit of the public interest. “Rent-seeking” and rent-protection are the order of the day. Because a proposal arguably in the public interest almost always serves someone’s private interest, it will not likely be entirely without a coalition of advocates. The WMD domain is probably no different than any other in these general ways. It differs from other domains, however, in that it is technically more difficult for would-be rational and public-spirited policy makers to make appropriate judgments. The probabilities of attack are too uncertain, the magnitude of negative outcomes too hard to contemplate, the efficacy of counter-strategies too hard to assess. Under these conditions, it is very easy for the manipulation of symbols about mass casualties and mass destruction – or, on the other side of the political divide, allegations of ethnocentric paranoia and fondness for fascism – to drive out rational discourse. On the demand side, then, policy learning in the WMD domain is probably a bit worse than average.

Putting our two assessments together, then, of supply and demand processes, learning in the WMD domain is probably very near the average for all policy domains. When compared to the standards we might reasonably hold forth, given the individual and collective stakes, this is not a good result.

8.7 Conclusion

We have considered several adaptive mechanisms bearing on the nation's response to terrorism in general and WMD in particular: mobilizing resources, using them wisely, building institutional capacity in the public sector, utilizing the strengths of the private sector, and learning by a variety of means. Despite the pitfalls, I have occasionally judged the adaptive response by reference to some absolute standard of performance. But more commonly, I have used a relative standard based on how WMD policy-making and policy implementation stacks up against similar processes in other areas of social and economic life.

The mainstream consensus among experts is that our mobilization of resources falls short, though probably not disastrously so. Such resources as we deploy are targeted about as well as government does such targeting generally. But spending and targeting money appears to be easier than building the needed institutional capacity – that is, fixing our public bureaucracies and getting them to

work together – and in this regard homeland security resembles government generally. The results on this institutional front so far are very troubling, though even more disturbing is our mediocre political capacity for learning what to do and acting on such learning.

Because so much is at stake, one might have hoped for better results. Is there a reasonable prospect for improvement in the near future? Let us leave aside whether the threat environment will grow better or worse because of such events as the war in Iraq or trends such as ideological developments in the Muslim world, and consider only our capacity and motivation to cope with this environment. We can, of course, expect slow and steady incremental improvements in our capacity to mount counter-measures, along the lines discussed in this chapter, e.g., using risk as a basis for resource allocation, or developing more effective detection techniques, or integrating local and federal intelligence operations. Our question, though, is whether these trends can accelerate. We must therefore consider what conditions bearing on these trends might be changing, either for the worse or the better.

One clear change for the better is in prospect, to wit, deceleration of the large-scale organizational transitions at the federal level and their ripple effects at state and local levels. Establishing the DHS and the DNI, and efforts to reorient

the FBI, are probably themselves a cause of lowered institutional capacity; and these transitions will conclude in due course, say five to ten years.

A more debatable set of changes concerns political and policy leadership and management skill, areas less discussed in this paper than institutional capacities and limitations but certainly of great importance. Leadership can to some degree be credited, for instance, when DNI Mike McConnell succeeds in creating a joint duty program for the Intelligence Community when earlier George Tenet had failed. Similarly, FEMA flourishes when Jamie Lee Witt heads the agency, with the full support of President Bill Clinton, but it declines when President George W. Bush allows it to be demoted to just another unit within the Department of Homeland Security.

Of course, leadership need not come only from the highest-level officials. Leadership is a type of activity. It can come from anyone, in any position, capable of seizing the opportunity and facilitating collective action towards a worthy collective goal. It need not be overt or dramatic; it can be subtle and stealthy. But even leaders have leaders. And it would help if the leaders in official, high, and visible positions were to exercise their powers on behalf of more policy rationality and more policy and implementation action directed

towards the public interest. In this regard WMD is very much like every other policy area in American government.

¹ It may be, as one well-respected political scientist has argued, that the absence of terrorist attacks on US soil since September 11 can be explained by the simple absence of individuals motivated to conduct them. (Mueller, 2006)

² A significant omission, for instance, is recalibrating the tradeoffs between security and privacy. I will simply note here that the intense and widespread debate over this matter is itself a matter for national self-congratulation, no matter one's views on how it is turning out.

³ Some might count the explosive in this case as a weapon of “mass disruption” rather than “destruction” because it would not pose hazards to responders or the public of the same sort that nuclear, chemical, biological, or radiological weapons do.

⁴ Of this, the Department of Homeland Security received about \$28 billion . The Brookings group adjusts for an accounting change that added Department of

Defense expenditures of \$17 billion to the 2007 figure in the administration budget.

⁵ State and local government additional spending on homeland security in excess of federal grant monies is not well documented. An estimate by Bart Hobijn in 2002, based on surveys of US governors and mayors, projected about \$2.9 billion per year in the near future, declining over time, as much of the expenditure was on capital investment. (Hobijn, 2002) Hobijn recently estimated private expenditures for the period 2001-2005 at a modest \$9.4 billion. However, he included expenditures only on security personnel and electronic protective systems. (Hobijn and Sager 2007) Certain sectors, such as transportation, would incur substantial private capital expenditures not included in Hobijn's estimates.

⁶ Note that it is not clear in these or in most popular discussions of domestic security expenditures what percentage of the cited amounts is one-time versus ongoing, though it appears from the context that most of it is ongoing.

⁷ Brzezinski is not himself necessarily identified with the *Mother Jones* left, having been a reporter for the *Wall Street Journal*.

⁸ This is an instance of what psychologists call a “framing effect. (Van Der Pligt, 1996)

⁹ The term “fiscal illusion” is more commonly used in the public finance literature, however, to indicate the opposite false belief: that more spending is all benefit and no cost. (Dollery and Worthington, 1996)

¹⁰ As for the short term, Carafano implies that the needed funds could come from money currently spent on wasteful strategies. The Century Fund panel proposed a menu of specific cuts in the Defense Department budget. The Brookings authors say nothing about how to finance their recommendations.

¹¹ Interestingly, a survey of city officials and state residents in California in 2003 showed that officials underestimated residents’ willingness to pay higher taxes in exchange for higher security. (Baldassare et al., 2003) Residents of large cities were considerably readier to pay more than were other residents.

¹² For an argument that assumes the opposite incentives for elected officials, however, see Sunstein (2006).

¹³ In Europe, the problem is on its way to a solution because policy-makers were able to build on a history of standardized frequencies linking law enforcement and emergency services across countries and to rely on the European Telecommunications Standards Institute's policy flexibility.

¹⁴ New York City pays for some intelligence agents stationed abroad, although so far the federal government has not agreed to share any of the cost.

¹⁵ Matthew Bunn offers what he calls "a plausible set of parameter values" and estimates a 29% probability of a nuclear terrorist attack by 2016. (Bunn 2006) His parameter values appear to incorporate only a moderate level of counter-measures.

¹⁶ Some technical arguments may be raised against investment but dismissed. It is true that terrorists can always shift their aim from a better protected target to a worse protected target. But forcing terrorists to attack "second choice" targets reduces the value of attacking in the first place. Secondly, any single defense can be penetrated by a clever and determined adversary. But there is value in partial defenses – "layering" or "defense in depth" – which

increases the odds that one of the defenses will work and, in any case, complicates terrorist calculations and execution strategies. (Flynn, 2004; Schneier, 2003)

¹⁷ The technical tests were also, apparently, tilted in favor of ASP by being biased against the status quo, namely, the PVT portal monitors. In addition, the DNDO violated the DHS guidelines for performing cost-benefit analyses, and seemingly relied on only 11 of at least 54 tests on commercially available portal monitors completed by the Department of Energy's national laboratories since September 11. (GAO, 2007c) The Congress subsequently halted DNDO's purchase pending further study. (Aloise, 2007)

¹⁸ Note that we are referring here to security, not safety.

¹⁹ Lee Clarke has pointed to the prevalence of "fantasy planning" in the emergency preparedness field. (Clarke 1999)

²⁰ I have in mind the Program Assessment and Rating Tool (PART). See the OMB web site <http://www.whitehouse.gov/omb/expectmore/index.html>.

²¹ In December 2006, the government canceled the contract with VaxGen, after the company had failed to meet a number of milestones.

²² See, for instance, House Committee on Government Reform (2006).

²³ In the White House white paper of February 2006, *The Federal Response to Katrina: Lessons Learned*, President Bush is quoted as saying that “four years after ...September the 11th, Americans have every right to expect a more effective response in a time of emergency. When the federal government fails to meet such an obligation, I, as President, am responsible for the problem, and for the solution” and “the system, at every level of government, was not well-coordinated, and was overwhelmed in the first few days.” (US, 2006)

²⁴ A different approach than using actual outcomes is to use specially constructed metrics that measure outputs or capabilities or some other corollary of actual performance. Such metrics would be useful for tracking institutional progress over time, say, on a year-to-year basis. These would be more evident to senior managers and policy makers than to members of the public, and some are already in use. See, for instance, the annual assessments made by the US Office of Management and Budget of the Department of Homeland Security at

<http://www.whitehouse.gov/omb/expectmore/agency/024.html>. Technical problems beset the design, collection, and use of relevant data – how do you measure whether an agency’s “analytic capacity” has increased or a Qaeda agent has decided not to attempt a border crossing? – but many creative possibilities are under discussion. (Caudle, 2005a,b; Caudle and Yim, 2006)

²⁵ She refers to the responsible factors as structure, incentives, and culture.

²⁶ There are also some valid technical objections to splitting law enforcement from domestic intelligence. (9/11 Commission, 2004)

²⁷ A year earlier the Public Discourse Project, a continuation of the September 11 Commission, published a follow-up document to their original (2004) report. They commented that the FBI’s “trend line” “has been in the right direction, but far too slow.” And “The FBI’s culture continues to resist Director Mueller’s changes.” (Public Discourse Project, 2005b)

²⁸ The GAO, in a 2004 report, said the “FBI has made significant progress in its transformation efforts since GAO last testified...in June 2003” but went on to

note the FBI's difficulties in retaining staff with intelligence knowledge, skills, and abilities. (GAO, 2004)

²⁹ That Goldwater-Nichols has actually been successful is generally accepted by close observers, though there are dissenters. There is some concern, for instance, that it has eroded civilian control and that it has suppressed useful criticism coming from the perspectives of the separate and rival military services. (Bourne, 1998) Also, it appears that "jointness" is used as an ideological hammer to enforce military services conformity to doctrinal change being advocated by the office of the Secretary of Defense. (Owens, 2006)

³⁰ Legal and political issues arising from our federal structure complicate matters (Leonard and Howitt 2006), as well as issues of how state and local government can coordinate the military in response to an event. (Lehr, 2006)

³¹ For a much more complex case involving the Ports of Los Angeles and Long Beach, see Zegart et al. (2006).

³² More generally on the "secret war" between the FBI and the CIA, see Riebling (2004).

³³ The ODNI competed in the annual Kennedy School of Government Innovations in Government program in 2008. The program reached the finalist round, which earned them a site visit. I was the assigned site visitor and, in that capacity, interviewed many enthusiastic line-level participants and program managers. An indication of high-level support is that the ceremony surrounding the issuance of implementing instructions featured the Secretaries of Treasury, Defense, and Homeland Security; the Chairman of the Joint Chiefs of Staff; and prominent deputy secretaries from State and Energy. These agencies had also signed a so-called “treaty” affirming support for the program and its implementing details.

³⁴ The Japanese were probably less ready to learn from the event than Americans would have been, since they resist acknowledging terrorism. Even after the sarin gas had been identified as such, police insisted it had been accidentally produced by a gardener mixing fertilizers. Pangi (2003).

³⁵ But this tendency is patchy and error-prone, sometimes under-reacting and sometimes over-reacting, although it appears that in the long run (years if not decades) learning does occur. (Morrall, 2003; Birkland, 2006).

.

³⁶ For a slightly cynical account of FEMA’s oscillation between a focus on security and an all-hazards approach, see Perrow (2006).

³⁷ “Joint Information Center,” “Joint Operations Center,” and “Disaster Mortuary Assistance teams,” respectively.

³⁸ Israel tests its disaster response system with non-simulated alerts, such as when residents of the North were sent to shelters in 2000 because of fears that Hizbullah would attack. The state of emergency lasted only 48 hours, but it revealed problems in distributing food and mattresses and in confining physicians to shelters when they were needed on the outside. (Merari 2003)

³⁹ Of course, attempts should be made to control for differences among sites unrelated to the practice(s) being evaluated.

⁴⁰ A GAO site search for “terrorism” or “WMD” for the period June 2006-May 2007 returned 1170 entries, about two-thirds of them reports. The 30-40 GAO products I have sampled in preparing this paper have been of very high quality.

⁴¹ The *Washington Post* editorialized on December 28, 2004: “There are 79 such panels; every single senator and at least 412 of the 435 House members have some degree of responsibility for homeland security operations. By contrast, the Defense Department, with a budget 10 times that of DHS, reports to ‘just’ 36 committees and subcommittees. ...From the perspective of national security, this fragmented, dysfunctional structure is sheer lunacy. Department officials spend too much time responding to their many congressional masters; last year alone, according to the departing secretary, Tom Ridge, he and other top department officials testified 145 times before various committees and subcommittees. Moreover, such balkanized oversight is less effective rather than more so, because members of Congress suffer from parochial viewpoints influenced by their individual committee assignments and fail to develop a broad overview of homeland security priorities.