Preparing for Catastrophic Bioterrorism

Toward a Long-Term Strategy for Limiting the Risk

Richard Danzig

Center for Technology and National Security Policy

May 2008

The views expressed in this article are those of the author and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. Government. All information and sources for this paper were drawn from unclassified materials.

Richard Danzig was Secretary of the Navy 1998–2001 and is a consultant on bioterrorism to the Defense Advanced Research Projects Agency and other Federal Agencies.

Acknowledgments. This paper is an updated version of a paper prepared in December 2005 for DARPA's Defense Sciences Office and benefits from insights from other projects undertaken for DARPA. I am particularly grateful for the support of DARPA's Defense Sciences Office and for the insights of Brett Giroir, Michael Goldblatt, and Steve Wax, directors of that office; to DARPA's Special Projects Office for support and for the insights of Amy Alving in a previous project relevant particularly to Part IVD; and to DARPA's Microsystems Technology Office for support and for the insights of John Carrano in a previous project relevant particularly to Part IVA. More broadly, I am also greatly indebted for comments on this paper from Michael Callahan (then at CIMIT now at DARPA), Gerald Epstein (Center for Strategic and International Studies), Dave Franz (Midwest Research Institute), Michael Hopmeier (Unconventional Concepts Inc.), Kendall Hoyt (Dartmouth Medical School), Tom Inglesby (Pittsburgh Center for Biosecurity), Bob Kadlec (White House Homeland Security Council), Josh Lederberg (Rockefeller University), Terry Leighton (Oakland Children's Hospital), Fred Leykam (The Washington Institute), David Relman (Stanford Medical School), Tara O'Toole (Pittsburgh Center for Biosecurity), Margaret Stock (The United States Military Academy), Jerry Warner (Defense Life Sciences Inc.), and John Vitko (Department of Homeland Security). I thank Margaret Cosentino, Aidan Kirby, Rachel Kleinfeld, and Andrew Tabler of the Center for Strategic and International Studies for fine research assistance. Finally, I am grateful to Hans Binnendijk (National Defense University) for encouraging this publication and to Bill Bode for his excellent editorial work.

Though I have greatly benefited from the advice and support of these people and institutions, I emphasize that the views presented are my own and should not be attributed to them.

Defense & Technology Papers are published by the National Defense University Center for Technology and National Security Policy, Fort Lesley J. McNair, Washington, DC. CTNSP publications are available online at http://www.ndu.edu/ctnsp/publications.html.

Contents

Introduction

Our national biodefense program—our program to defend Americans at home and abroad against the use of bacteria, viruses, toxins, and neuro-modulators as weapons—is an agglomeration of tactics presented as a strategy.[1] Because we do not have a true strategy, our efforts are afflicted by three kinds of failure.

First, we suffer from critical gaps, disconnects, and an absence of synergies, both within our Federal bureaucracies and between our Federal government and state, local, and foreign governments.

Second, we are not effectively engaging the public (whose acceptance, attitudes, and actions are crucial to preparing for and responding to attacks) and private industry (where drug and defense companies in particular can offer much-needed skills and resources).

Third, we have not created mechanisms of discussion and decision that are robust enough to build consensus, illuminate difficulties, and allocate responsibilities for overcoming these difficulties.

Many things are required to correct those failings, but I believe that four are fundamental. We must:

- articulate how bioterrorism fits into an overarching concept of terrorism;[2]
- identify characteristics of bioterrorism that imperil our national security;[3]
- build our initiatives around these characteristics rather than, as at present, largely ignoring them—we now allocate our energies and resources largely in response to bureaucratic and

[1] The most complete articulation of our present strategy is Homeland Security Presidential Directive 10, "Biodefense for the 21st Century" (April 28, 2004), available at <http://www.whitehouse.gov/homeland/20040430.html>. It catalogs a biodefense program built on four "pillars:" "threat awareness" (by developing intelligence and undertaking assessments, including efforts to anticipate future threats), "prevent and protect" (through diplomacy, interdiction, and critical infrastructure protection), "surveillance and detection" (through attack warning and attribution) and "respond and recover" (through response planning, risk communication, medical counter-measures, mass casualty care, and decontamination). Though useful, HSPD-10 is a catalog of desired activities, not a strategy.

Overarching documents outlining the Administration's war on terror include the President's September 28, 2005 statement "Fighting a Global War on Terror," available at <www.whitehouse.gov.news/releases/2005/09/images/20050928_p092805pm-0055jpg-515h.html>, and the 2003 *National Strategy for Combating Terrorism*, available at <whitehouse.gov.news/releases/2003/02/20030214-7.html>. These documents emphasize fighting terrorists abroad, denying state support or state control for terrorists, preventing access to weapons of mass destruction, and expanding democracy in the Middle East.

[2] This paper addresses issues of defense against terrorist use of biological weapons. Though I regard this as our primary risk of biological attack, there are reasons to be concerned, as well, about state-sponsored biological attack or criminal use of biological weapons. Some of these may differ from terror attacks either in the desire of their perpetrators to keep the attack secret (see footnote 106) or because, in common parlance, we do not regard state actors or those who seek financial rather than political reward as terrorists.

[3] This will also require a new vocabulary, parts of which I suggest in this paper. Ultimately, it will also demand improved methods of measurement and evaluation, which I do not address in this paper.

political competitions, pressure from professional and contractor interests, and the attractions of incremental opportunities for technology growth; and
- develop an organization and processes that will transcend the tendencies of participants in biodefense work to pursue separate agendas—these cannot be eradicated, but they can be orchestrated.

This paper, circulated within government early in 2006, outlines an approach to these requirements and provides several examples of how the application of this approach can create a strategy.[4] As described below, several of the recommendations offered here have recently been acted upon, some of them encouraged by this work, others as a consequence of independent, parallel initiatives. Nonetheless, more than 6 years—a period longer than World War II—after the 2001 anthrax letters catalyzed greater government efforts to counter bioterrorism,[5] our homeland security officials are still struggling to define a biodefense strategy. This paper is being published in the hope that a broader discussion will yield further progress.[6]

[4] In particular, in this paper I do not attempt to address international issues and most aspects of involving private industry.

[5] Prior efforts are well described in Judith Miller, Stephen Engelberg, and William Broad, *Germs: Biological Weapons and America's Secret War* (New York: Simon & Schuster, 2001), which, coincidentally, was published at the time of the 2001 anthrax letters.

[6] A beloved philosopher had this to say on the experience of ventilating one's ideas: "Pooh began to feel a little more comfortable, because when you are a Bear of Very Little Brain, and you Think of Things, you find sometimes that a Thing which seemed very Thingish inside you is quite different when it gets out into the open and has other people looking at it." A.A. Milne, *The House at Pooh Corner*, chapter six.

CHAPTER ONE

How Bioterrorism Fits in "The War on Terror"

The terrorist attacks of September 11, 2001, brought together two related but distinct phenomena. First, they presented the calling card of Al-Qaeda and more generally of militant Islam—these attacks were rightly perceived as an act of war by a group seeking to catalyze a political-religious movement. Much of America's effort since then has been to destroy that group, its sanctuaries, and its affiliates; some of the effort has been to counter the psychological, social, and political appeal of aggressive (predominantly Wahabi) Islam.

Second, these attacks introduced the public to a more general phenomenon—our vulnerability to acts of terror on a greater scale than anything America had experienced. It is remarkable that in the turbulent 20th century, which witnessed some 200 million deaths from politically driven violence and war, no single attack on American soil equaled the estimated 3,000 deaths on 9/11.[7] The implications for America are the graver because the capability to inflict carnage at this level—and at much higher levels—is not confined to a group or movement. It lies at hand as an instrument that can be used by any belligerent group (or state, or individual). It will survive the destruction of Al-Qaeda and the abandonment of jihad.

These two strands of war—jihadi terrorism and our general vulnerability to terror on a large scale—intertwine but are independent. The tendency to confuse them is accentuated when policymakers rhetorically jump from one to the other. The effect resembles one produced by the thaumatrope, a popular 19th-century toy now encountered only as a curiosity.[8] A horse is depicted on one side of a disk or card and a man on the other, or a cage on one side and a bird on the other. When the object is spun quickly the rider appears on the horse, or the bird in the cage. Our inability to separate images shown us in rapid succession merges the two in our minds.

We speak of a "war on terror" (not just on Al-Qaeda) and have devoted significant resources to controlling and preparing for the consequences of "weapons of mass destruction," but these efforts overwhelmingly focus on the present challenge of jihadi fundamentalism. Our inherent vulnerability to large-scale terrorism is more troubling but less addressed.

Starkly contrasting statements made by the President half a day apart indicate the difficulty of disentangling the two strands. On the "Today Show" on the night of August 30, 2004, President Bush was asked when the war on terror would end. His answer was that it had no end. The next morning, responding to a political uproar, the President told the American Legion that the war could and would be won. The second statement is correct if we think of this as a war on Al-Qaeda or against militant jihadis. The first statement is correct if we think of this as a war against terror, because

[7] The Japanese attack on Pearl Harbor produced 2,403 deaths. In the 19th century, some Civil War battles exceeded 50,000 deaths. See <www.civilwarhome.com/Battles.htm>. As noted in section V, not even natural disasters were as deadly.

[8] I am indebted to the late Leon Lipson for this metaphor.

neither the instrument of terror nor our vulnerability to terrorism can be eradicated. Confusion arises from the application of the same term to two different phenomena.

A sounder approach would rigorously distinguish between the two strands. Al-Qaeda and its allies and affiliates are a *threat* that can be (and probably will be) eradicated; with respect to the broader movement, we will find a means of reconciliation. Our vulnerability to the use of biological, chemical, radiological, nuclear, and other mechanisms for creating terror is a *risk*. The risk cannot be eliminated. To the contrary, it is likely to grow as technologies proliferate. To cope with this problem, we must find a strategy of *risk management*.

Al-Qaeda can be pursued with familiar instruments and through established organizations (particularly our Department of Defense and our intelligence agencies). Applying well-developed professional skills in a new context, our national security establishment is moving toward a consensus view of the *threat* posted by terrorist groups, broadly useful models of how they are financed, organized, recruit, train, and plan, and a set of theories about how to counter these activities over the next few years.[9] The enduring *risks*, by contrast, demand original strategic thinking, rather as nuclear weapons (not just the Communist threat) demanded and elicited new paradigms in the decade after World War II. We do not yet have that body of new thinking.

There is an important difference in the time dimensions in which we should think about the two strands. Current thinking about Al Qaeda (the first strand) is focused on what can fairly be described as a clear and present danger. The second strand (our broader and more enduring vulnerability to the proliferation of the means of terrorism) is not clear and present; it is obscure, questioned by some, and more dangerous in the future than now. The concept of a war on terror is misleading when applied to the second strand of enduring risks. A war is a state of emergency in which an opponent is defined, tactical initiatives are imperative, and "strategies" are plans for this year, the next one, and maybe the year after. A long-term risk requires long-term plans and long-term solutions against a range of unidentified (and often unpredictable) opponents and weapons.

It was sometimes said about our experience in Vietnam that, though we fought for a decade, we conducted not a 10-year war, but ten 1-year wars. We must avoid replicating this failure in our battles against the new means of terrorism. If we accept that our risk from the proliferation of the means of terrorism is broad and enduring, then, though these means certainly pose a near-term challenge, they demand a strategy with a longer time horizon.

---

[9] An early description may be found in *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, (Washington, DC: Government Printing Office, 2004), 169–173. There are, of course, differences in view still being debated. Compare for example, Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004) (setting forth essentially a secular view of recruitment by establishing social alternatives to alienation) with Stephen P. Lambert, *Y: The Sources of Islamic Revolutionary Conduct* (Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, 2005) (ascribing recruitment dominantly to religious motivations).

CHAPTER TWO

Bioterrorism in the Context of Risk Shifting, Escalation, and Contagion

Bioterrorism is not now a prevalent means of terrorist attack. Incidents are sparse, involve a fraction of a percent of all attacks,[10] and have not produced large numbers of casualties, although the anthrax letters in 2001 had substantial economic consequences. A long-term strategy requires an underlying judgment about the probability of this changing and of the speed with which change is likely to occur. If we are very confident that change is unlikely, we ought not to invest substantially against this risk; if we choose to invest but think the change will come slowly, giving us time to adjust, then we can defer many investments until we find that we need them.

Assessing the Risk

I believe that we do not have a basis for judgment about when bioterrorism will be inflicted upon us. A major bioterrorist attack could occur tomorrow (indeed, might have occurred yesterday without our knowing it) or may be deferred for many years. Recognizing this unpredictability, I favor an investment portfolio that is balanced between near- and long-term improvements in our protection. But I assess the risk as significant and growing. As the technologies of modern biology (and related fields of aerosol spraying and material preparation) have proliferated, continue to proliferate, and will predictably proliferate further, so have the technologies of bioterrorism. In critical respects, they are one and the same.[11] Unfortunately, offensive capabilities can be developed more quickly than defenses against them. Developing vaccines, methods of detection, and methods of physical protection against particular pathogens or classes of pathogens, for example, requires more lead time than does the capacity to grow and effectively distribute those pathogens.

Another aspect of our risk demands attention, but does not receive it. We need a *theory of diffusion* applicable to all instruments of terrorism (including, for example, airplane hijacking, suicide bombing, and cell phone-triggered improvised explosive devices, as well as bioterrorism).

When we adopt a long-term perspective, it is evident that the war on terror will have to cope with numerous enemies. Some of these will be tightly coordinated with one another, some will be loosely coordinated, some will operate wholly independently, and some do not yet exist. (The first three varieties are illustrated by the differences in relation to Al-Qaeda of the 9/11 attackers, Iraqi

[10] Aaron J. Clauset and Maxwell Young, "Scale Invariance in Global Terrorism," *Physical Review E* 73, 026130 (2006), calculate that between 1975 and 2004, only 0.4 percent of terrorist attacks involved biological or chemical weapons.

[11] I comment on the intertwining of these technologies in the discussion of our intelligence challenges in part VI.

insurgents, and the 2004 Madrid bombers: the first were directed, the second are aided, and the third probably merely inspired.) At the foundation of our strategy, a theory of diffusion should explain and predict the process by which goals, technologies, and concepts of operation pass from one or a few to many of these opponents.

Three Aspects of Risk

Any instrument of terror can lie latent for a substantial period and then become widely employed. The risks of the use of a weapon or class of weapons rise with the increase in numbers, commitment, or desperation of terrorists. Choices of instruments will be affected by terrorists' resources, knowledge, desired effects, and judgments about a target's strengths and vulnerabilities. Driven by these factors, we are likely to experience *risk shifting*, *risk escalation*, and *risk contagion*.

Risk shifting can be expected if the demand for instruments of terror remains, but prevalent instruments become less effective means of achieving terrorists' ends. When a tactic becomes so familiar that it no longer produces the headlines a terrorist desires, we are likely to experience a risk shift. Bruce Hoffman has observed this phenomenon:

> There appears to be a pattern that suggests that at least some terrorists have come to believe that attention is no longer as readily obtained as it once was. To their minds, both the public and the media have become increasingly inured or desensitized to the continuing spiral of terrorist violence. Accordingly, these terrorists feel themselves pushed to undertake ever more dramatic or destructively lethal deeds today in order to achieve the same effect that a less ambitious or bloody action may have had in the past … This equation of publicity and carnage with attention and success thus has the effect of locking some terrorists into an unrelenting spiral of violence to retain the media and public's interest.[12]

Warfare is a form of co-evolution. Many observers have noted that terrorists adapt to our successes.[13] It is commonplace, for example, to describe our opponents in Iraq as "a thinking enemy," "an adaptive enemy," or "an evolving enemy," and to expect to be confronted by new tactics and techniques as we render old ones less effective.

Our planning, however, seems remarkably obtuse about the likelihood of larger shifts to new classes of weapons.[14] This leads to an under-emphasis on planning for bioterrorism—a weapons area that will be particularly attractive to terrorists because we are not yet capable of mounting strong defenses against it. Moreover, bioterrorism's capabilities for *reload* and *large-scale catastrophic effects* (both described below) are likely to make the use of pathogens not simply a risk shift, but a risk esca-

---

[12] Bruce Hoffman, "Terrorism Trends and Prospects" in Ian O. Lesser et al., *Countering the New Terrorism* (Santa Monica: RAND, 1999), 13.

[13] A classic analysis around moves and counter-moves relating to hostage taking is Martha Crenshaw, "The Counter-Terrorism and Terrorism Dynamic," in ed. Alan Thompson, *Terrorism and the 2000 Olympics* (Canberra: Australian Defence Studies Centre, 1996) 125ff. Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1999), 180–182, describes the IRA's tactical adaptations to British Ministry of Defence electronic countermeasures from the 1970s through the 1990s. He concludes that the pattern is one of "persistent search for new ways to overcome or circumvent or defeat governmental security or counter-measures … [a] relentless quest … [that] illustrates the professional evolution and increasing operational sophistication of a terrorist group," 180.

[14] For a good exception, see Raphael Perl, "Combating Terrorism: The Challenge of Measuring Effectiveness," CRS Report for Congress RL33160 (Washington, DC: Congressional Research Service, November 23, 2005): "it is important not only to measure where terrorism is, but also how close terrorists are to the next quantum jump. The potential quantum jump currently of greatest concern to many would be to WMD (chemical, biological, or radiological/nuclear)," 7.

lation; biological weapons will inflict more damage than the more mundane weapons they will replace. And of the potentially catastrophic weapons, they are the most easily acquired.[15]

Risk escalation toward bioterrorism particularly demands planning attention, because it may come upon us not by stages but suddenly. Some instruments of terror evolve slowly, but others respond to attributes of fashion and are subject to tipping points,[16] cascades,[17] inspiration by example,[18] and proliferation from cutting edge innovators who disseminate technological and tactical ideas. To invoke a biological metaphor, some instruments used in attacks rapidly become endemic; a few are highly contagious.[19]

Risk contagion occurs when Internet, television, press, pamphlet, and oral reporting highlight the attraction of a previously little-used instrument;[20] lead users perfect this instrument;[21] barriers to entry diminish as legitimate and illicit information proliferates about how to build these weapons and

---

[15] Many have rightly emphasized the dangers from potential terrorist access to nuclear weapons. See, for example, Graham Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (New York: Times Books, 2004), 67–86, Matthew Bunn and Anthony Wier, *Securing the Bomb 2005: The New Global Imperatives* (Washington, DC: Belfer Center, 2005), 27–40. As these sources suggest, however, this problem is subject to a degree of control by more extensive security efforts. Biological resources are vastly more widely dispersed and accessible than nuclear bombs.

[16] See generally Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference* (New York: Little Brown and Company, 2000), 2, 4: "…think of them as epidemics. Ideas and products and messages and behaviors spread just like viruses do…. [C]hange happens not gradually but at one dramatic moment …" Gladwell's book, written for laymen, roots in more precise social science research. Note particularly the sociology articles he references, 261.

[17] See generally James Surowiecki, *The Wisdom of Crowds: Why the Many are Smarter than the Few and How Collective Wisdom Shapes Business, Economies, Societies, and Nations* (New York: Random House, 2004), especially 55, 57, 59: "Do cascades exist? Without a doubt…. There are plenty of occasions when people do closely observe the action of others before making their own decisions. In those cases, cascades are possible, even likely…. Effectively speaking, a few influential people—either because they happened to go first, or because they have particular skills and fill particular holes in people's social networks—determine the course of the cascade. In a cascade, people's decisions are not made independently but are profoundly influenced—in some cases even determined—by those around them…. Mimicry is so central to the way we live that economist Herbert Simon speculated that humans were genetically predisposed to be imitation machines." Surowiecki observes, however, that "the more important the decision, the less likely a cascade is to take hold," 63.

[18] The copycat phenomenon is well known to criminologists. See, for example, Ray Surette, "Self-Reported Copycat Crime Among a Population of Serious and Violent Juvenile Offenders," *Crime & Delinquency* 48, no. 1 (January 2002), 46–69. One-fourth of violent male juvenile offenders reported attempting a copycat crime. Of course, it may be objected that demonstrations (for example, the anthrax letters) already existed, but have not triggered a tipping point. It is common, however, for multiple demonstrations to be required before a widespread response is triggered. Gladwell notes that "[t]here is a maxim in the advertising business that an advertisement has to be seen at least six times before anyone will remember it." Gladwell, *Tipping Point,* 92.

[19] The metaphor implies that they also will eventually slow, as the epidemic burns itself out. A study of race riots suggests, "because we know the riot rate increases during the first half of the riot wave and decreases during the second half, it is somewhat implausible to suggest that a linear relationship between infectiousness and the riot hazard exists. As a result, I hypothesize that infectiousness may have a curvilinear effect on the riot hazard. The logic of this hypothesis follows from classic diffusion models in which the rate of adoption is slow at the beginning of the cycle, peaks in the middle of the cycle, and then returns to near zero toward the end of the wave." Daniel Myers, "The Diffusion of Collective Violence: Infectiousness, Susceptibility and Mass Media Networks" *American Journal of Sociology* 106, no. 1 (July 2000), 184. Myers' data indicate that "analyses of rioting that fail to incorporate diffusion notions are seriously misplaced," 200.

[20] Daniel Benjamin and Steven Simon, *The Next Attack: The Failure of the War on Terror and a Strategy for Getting it Right* (New York: Times Books, 2005), 64: "The abduction and murder of *Wall Street Journal* reporter Daniel Pearl in January 2002 made decapitation virtually de rigueur in jihadist killings of individuals or small groups. Pearl's murder was videotaped, copies were widely sold, and it was posted on the Internet. The market for such carnage has exploded since then." This is consistent with Daniel Myers' observations about race rioting: " … people start discussing it … These conversations occur not only on an informal personal basis, but also more systematically via news coverage and editorials…. In effect, the opportunity to debate these questions, informally and publicly, allows individuals to signal their level of willingness to participate," 177.

[21] On this phenomenon in commercial contexts, see Eric von Hippel, *Democratizing Innovation* (Boston: MIT Press, 2005), particularly chapter 7, "Innovation Communities."

conduct these operations; the materials required for this instrument become accessible; and risk-averse attackers come to believe that the instrument can be relied upon.[22] As a result, a problem that was relatively rare and episodic breaks out and becomes chronic. Improvised explosive devices, suicide bombings, beheadings,[23] airplane hijackings,[24] and attacks on tourists all spiked quickly from low to much higher levels of incidence; a graph of suicide bombings and attacks against tourists illustrates the phenomenon. Frequencies in the past are not reliable predictors of frequency in the future.[25]

In unclassified publications, credible observers report that some cutting-edge perpetrators of terrorism are pursuing capabilities to produce biological weapons. But the demonstration and diffusion that would make this form of terrorism popular have not yet occurred. When the Japanese cult Aum Shinrikyo experimented with anthrax before turning to sarin, they fortunately (and presumably erroneously) used a vaccine strain that rendered their test harmless.[26] For reasons that are not clear, the perpetrator of the anthrax letters warned victims and thereby kept the death toll low. He (or she, or they) also stopped when he (or she, or they) may have been able to continue. Neither of these perpetrators used the Internet or other means to disseminate their techniques and pass them to others.

No one can calculate when a bioterrorism breakout will occur. We are all bad predictors of nonlinear events.[27] Even in retrospect it is hard to say why certain phenomena (the popularity of the hula hoop, the sky-rocketing price of oil, the bursting of the Internet bubble) matured when they did. But we can see that the ingredients for a bioterrorism breakout are there. The anthrax letters, Aum, and the reported efforts of Al-Qaeda are warning signs, directing our attention to the incipient danger.

The minimal scale and effects of attacks to date are sometimes advanced as arguments against spending scarce dollars and energies countering bioterrorism. The possibility of risk escalation leads me to the opposite conclusion: at the moment, bioterrorism is latent inside our system, but the infection has not yet multiplied to the point where it is substantially symptomatic. A long-term strategy for dealing with bioterrorism is imperative.

---

[22] The Congressional report on 9/11, House-Senate Joint Inquiry Report on 9/11," reprinted in *The 9/11 Investigations: Staff Reports of the 9/11 Commission*, ed. Steven Strasser (New York: PublicAffairs, 2004), astutely observed that "most terrorists are conservative in their methods," and that the danger of Al-Qaeda is rooted in large measure in its inclination for innovation. I comment on this further in part VI.

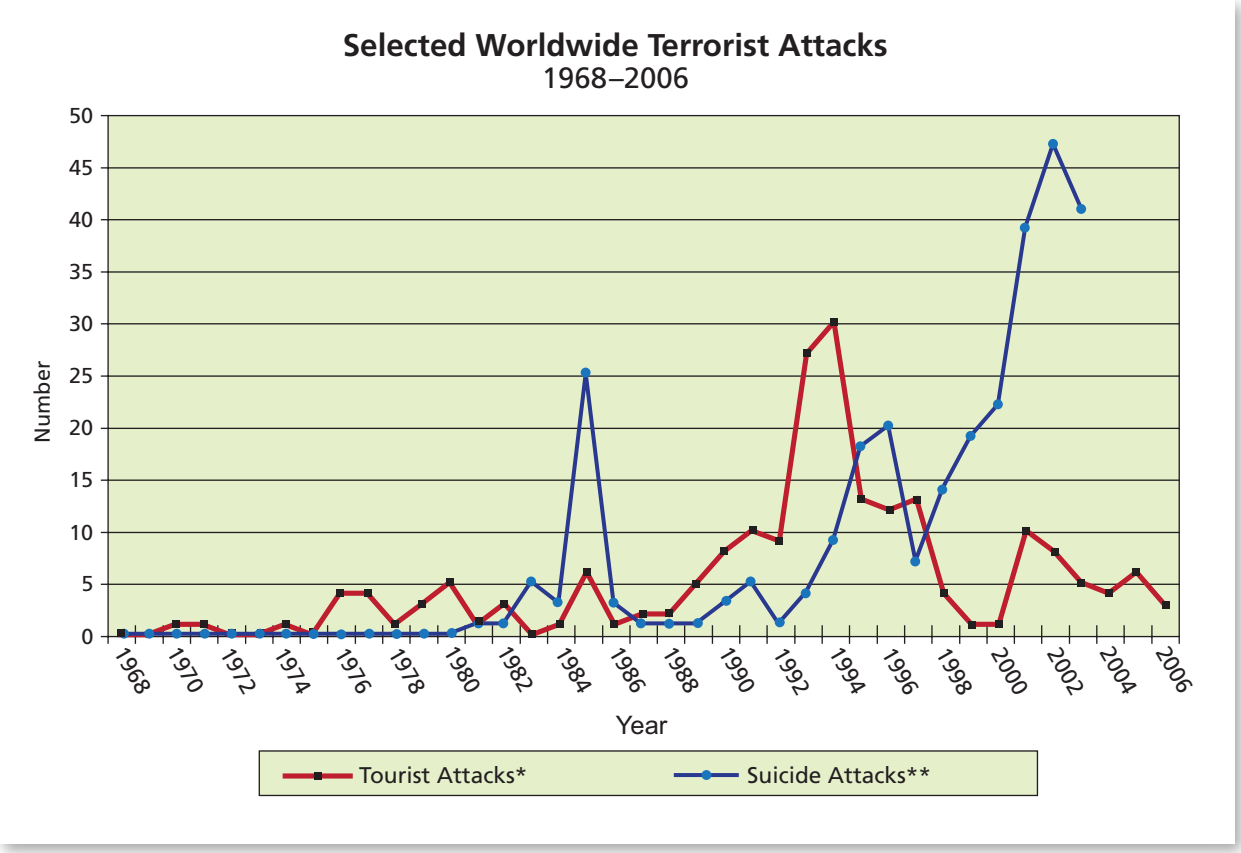
[23] Benjamin and Simon, 63–65, particularly 65: "Given the popularity and the sense that beheading is what a jihadist does, the spread of the tactic to countries beyond Iraq was inevitable."

[24] See generally Robert T. Holden, "The Contagiousness of Aircraft Hijacking," *American Journal of Sociology* 91, no. 4 (1986), 874–904. The first commercial airline hijacking occurred in 1948. Over the next 2 decades, the number of hijackings was low. The majority of hijackings were efforts to achieve refugee escapes. In 1969, Palestinians adapted this technique in an effort to force Israel to release political prisoners. "There were 82 recorded hijack attempts worldwide, more than twice the total attempts for the whole period 1947–67." <http://en.wikipedia.org/wiki/Aircraft_hijacking>. How Siang Meng, Director of Singapore's Counter-Terrorism Strategic Development Directorate, observes that a 1993 airplane hijacking by Chinese nationals seeking to escape to Taiwan "led to six similar hijackings in the next seven months" and argues that biological and chemical attacks will similarly proliferate. "The Chem-Bio Threat Assessed," *Pointer: Journal of the Singapore Armed Forces* 26, no. 4 (October–December 2000).

[25] The frequency of terrorism in general is another manifestation of fashion. "The census data for 1975 and 2005 indicates that the global population roughly doubled over this period, yet the frequency of terrorist events increased by more than a factor of ten," Clauset and Young, "Scale Invariance," 5. The authors point out, however, that some of this change may be a consequence of changes in our methods of recording incidents.

[26] Paul Keim et al., "Molecular Investigation of the Aum Shinrikyo Anthrax Release in Kameido, Japan, *Journal of Clinical Microbiology* 39, no. 13 (December 2001), 4566–4567, and Hiroshi Takashi et al., "*Bacillus anthracis* Incident, Kameido, Tokyo, 1993," *Emerging Infectious Diseases* 10, no. 1 (January 2004), 117–120.

[27] See generally Charles Doran, "Why Forecasts Fail: The Limits and Potential of Forecasting in International Relations and Economics," *International Studies Review* 1 (Summer, 1999), 11.



* Numbers of terrorist attacks on tourists were provided by the National Memorial Institute for the Prevention of Terrorism (MIPT), Oklahoma City, OK. Data and charts on terrorist attacks are available online from the MIPT Terrorism Knowledge Base Incident Analysis Wizard: Incidents by Target: Tourists 1968–2005, accessed at <www.tkb.org/AnalyticalTools.jsp>.[28]

** Number of suicide attacks is drawn from tables in Robert Pape, *Dying to Win: The Strategic Logic of Suicide Terrorism* (New York: Random House, 2005), appendix I, 253–264.[29] The Pape tables are arranged in 18 "campaigns" and include 20 attacks conducted in Iraq from March 22 to December 16, 2003. Those 20 attacks are omitted from this chart.

[28] I am indebted to Aidan Kirby of the Center for Strategic and International Studies for pointing me to MIPT, which makes such data available online, and to MIPT librarian Brad Robison for taking the trouble to generate an Excel chart suitable for printing.

[29] Appendix I lists 315 attacks conducted in the course of 18 terrorist suicide bombing campaigns, plus 14 isolated incidents. I am indebted to Andrew Tabler, then of the Center for Strategic and International Studies, for converting this data into a graph.

CHAPTER THREE

Recognizing Strategic Problems, Producing Strategic Responses

It is hard for any institution, and especially institutions at war, and most especially a democracy (even when at peace) to develop a long-term strategy. The task is conceptually hard and fraught with risk, and few people in responsible positions have the time or taste to develop concepts, much less to integrate them into a strategy. When they strive to develop a strategic perspective, our political leaders and public are more likely to look to the past (for example, who is to blame for 9/11) and the present (the most immediate crisis) than to invest in the future. Moreover, the engines of action in a democratic society—constituencies and interest groups—focus on their members' concerns and care most about near-term funding. Similarly, our bureaucracies are less devoted to setting priorities for solving problems than they are to competing for budget resources. Finally, outside the Department of Defense, the culture of strategic planning is not well established, and across our often competing bureaucracies there are only the weakest of integration mechanisms.

Digging Out of a Deep Hole

These problems afflict the war on terror generally. They are compounded by some special considerations affecting bioterrorism. After we quite properly renounced biological weapons almost 4 decades ago, we should have recognized that the absence of offensive thinking would handicap our defensive understanding[30] and therefore redoubled our defensive efforts. Instead, we persuaded ourselves that all others would act as we acted. We allowed our defensive expertise to erode and swept the problem under the rug. As a result, while our knowledge of nuclear, chemical, and explosive devices is rich, much of our knowledge about the weaponization of pathogens is dated. After 9/11, our initial thinking about bioterrorism was misconstructed around the agents, technologies, procedures, and priorities we worked with in the 1960s.

Our defensive preparations for bioterrorism also suffer from the confusions and controversies spurred by our extraordinarily complex, overtaxed, and widely criticized health care systems, and by the fragmentation of these systems between the Federal, state, local, and private entities throughout

[30] See Jeffrey W. Legro, "Military Culture and Inadvertent Escalation in World War II," *International Security* 18, no. 4 (Spring 1994), 108–142 describing, for example, how our limited offensive submarine program left us unprepared for imaginative German use of U-boats. In 1919, the Holland Committee on Chemical Warfare observed that: "… it is impossible to divorce the study of defence against gas from the study of the use of gas as an offensive weapon, as the efficiency of the defence depends entirely on an accurate knowledge as to what progress is being made or is likely to be made in the offensive use of this weapon." *Report of the Committee on Chemical Warfare Organization* ("Holland Committee Report"), submitted to the U.K. Parliament July 7, 1919, 5.

the United States. As has been well observed, "[t]he nation's health security cannot be built on a foundation of fragmented public health capabilities and capacities any more than our military could be effectively organized as thousands of independent militias."[31] Additionally, financial, historical, and psychological considerations keep our pharmaceutical companies, the biotech industry, and academic biologists outside our national security establishment. While physicists, chemists, and computer and telecommunications experts and enterprises abound in and around the United States government, we have not achieved similar cooperation with biologists. Finally, while we benefit from promoting consideration of bioterrorism by experts from related fields (infectious disease specialists, microbiologists, public health officials, emergency responders, etc.), we lack a discipline and even a vocabulary[32] to create a common focus on countering bioterrorism.[33]

Moving Beyond Rhetoric, Redoubled Funding, and Reorganization as Substitutes for Strategy

Responding to this complex of problems, we have resorted to three hollow tactics, each more dramatic and more irrelevant than its predecessor. These tactics—phony priorities—are pervasive in any system under stress. First, when confronted with the new problem we *relabel* what we have been doing and, under the new label, continue to do it. Then, as our sense of urgency intensifies, we allocate increasing amounts of money to the problem,[34] *redoubling* the pace at which we travel in diverse and only marginally productive directions. Finally, we *reorganize*, thinking that by establishing departments, directorates, commissions, and committees that bear its name we are addressing the problem.

Moving beyond this dysfunctional pattern is difficult. Those who do so make more substantive contributions than the relabelers, the redoublers, and the reorganizers. But, typically, our first substantive efforts grapple with second-order details rather than develop concepts that can provide a basis for strategies. A common way of developing these concepts is to catalog vulnerabilities and seek

---

[31] Elin Gursky, "Epidemic Proportions: Building National Public Health Capabilities to Meet National Security Threats: Report to the Subcommittee on Bioterrorism and Public Health Preparedness, Senate Committee on Health, Education, Labor and Pensions" (2005), 2, available at <http://www.homelandsecurity.org/journal/Epidemic_Proportions_2.pdf>. Gursky also observes: "Public health is organized to serve the health of individual communities with populations in the thousands, not the coordinated health security of a nation of 280 million. The country's public health departments are products of federalism …. We have no national health information system that streams medical and hospital data to public health departments …," 1.

[32] Some new terminology is suggested in this paper.

[33] This difficulty is exacerbated by the variety of forms of potential biological attack, from individual to mass attacks; in agricultural, urban, or international settings; against economic, symbolic, or human targets.

[34] It is difficult to tally our investments against terrorism generally and bioterrorism particularly. Besides raw budget numbers, The Office of Management and Budget annually publishes a pamphlet of "Analytic Perspectives" summarizing the Federal budget according to "mission areas," but these are categories like "intelligence and warning," "border and transportation security," and "defending against catastrophic threats." To arrive at a general estimate of bioterrorism-related funding, I would begin by noting order-of-magnitude differences in three components of the Administration's FY 06 budget: $442 billion for the Department of Defense, $41.1 billion for the Department of Homeland Security, and $4.4 billion for homeland security activities (essentially bioterrorism defense) in the Department of Health and Human Services. Steven Kosiak, "Overview of the Administration's FY 06 Request for Homeland Security," Center for Strategic and Budgetary Assessments, May 2005, available at <http://www.csbaonline.org/4Publications/PubLibrary/R.20050517.FY06Bud/R.20050517.FY06Bud.pdf>. (I have rounded Kosiak's more precise numbers.) Of course, these top-line organizational categories (the clearest ways in which we track spending) are not equivalent to functional categories. Kosiak goes on to estimate total Homeland Security spending at $50 billion. My rough estimate is that if bioterror spending in DHS, DOD, EPA, and elsewhere were enumerated it would equal the HHS number. This would bring total biodefense spending to around $9 billion per year (others have produced estimates between $6 billion and $14 billion). As a rough estimate, bioterrorism receives some 15–20 percent of the homeland security total and 1–2 percent of our total security spending.

one-to-one solutions to them. In the war against terrorism generally, for example, many of those concerned with protecting infrastructure pursue this approach when they enumerate dams, nuclear plants, monuments, etc. that must be defended. In bioterrorism, the equivalent effort, undertaken by the Department of Homeland Security's National Biodefense Analysis and Countermeasures Center (NBACC), was to assemble experts to rank pathogens according to the threats they are perceived to pose. This approach led to substantial work by the National Institute of Allergy and Infectious Diseases to develop an improved vaccine against anthrax. Generally, however, the effort has encountered many frustrations and been much criticized. As we will see, even if it succeeded it could not be the foundation of a broader strategy; there are too many potential agents, and their use is too unpredictable to support extrapolations of this approach.

Identifying Attributes

An alternative mode of analysis identifies functional difficulties and tries to address those. We suffer from minimal abilities to control or limit the damage from misuse of pathogens, know-how, and equipment because:

- pathogens occur naturally (it is as if we were attempting gun control while guns grew on trees),
- biological weapons can be produced, stored, and disseminated using now-widespread commercial and academic technologies and tools,[35]
- the relatively low threshold to achieve a bioterrorism capability threatens to empower individuals (for example, a biological Unabomber[36]) in a manner previously associated only with well-funded groups and states,
- a continuing, exponential acceleration in knowledge of biology and aerosol dissemination is likely to increase future risks of bioterrorism,
- we have substantial difficulties detecting production facilities (these can be as small as a room), stockpiles (kilos can disrupt multiple cities), and attacks (it usually takes hours or days to know an attack has occurred and natural events and errors give rise to false positives),
- we have inadequate methods of physical protection against many pathogens (by contrast, we commonly reinforce walls and windows to thwart explosions, but barriers to pathogens are expensive and at best partially effective—in some cases none exist),

---

[35] See generally Gerald L. Epstein, *Global Evolution of Dual-Use Biotechnology* (Washington, DC: Center for Strategic and International Studies, 2005).

[36] With regard to the motivations of lone attackers, see R.A. Fein and B. Vossekuil, "Assassination in the United States: An Operational Study of Recent Assassins, Attackers and Near Lethal Approachers," *Journal of Forensic Sciences* 44, no. 2 (March 1999), 321, analyzing characteristics of 83 people who since 1949 attacked or approached "a prominent person of public status in the United States." On the Unabomber, see Alston Chase, *A Mind for Murder: The Education of the Unabomber and the Origins of Modern Terrorism* (New York: W. W. Norton & Company, 2004) and, for commentary on the Unabomber as an example of a larger class, see Ron Arnold, *Ecoterror: The Violent Agenda to Save Nature* (Bellevue, WA: Merril Press, 1997). Unfortunately, even if loners were regarded as irrational or psychotic (a doubtful proposition), the literature suggests that this is not incompatible with capability. See John L. Karlson, "Psychosis and Academic Performance," *British Journal of Psychiatry* 184, no. 4 (1994), 327–329, reporting that psychosis was *over-represented* in those who finished first in high schools in Iceland. And see Armand M. Nicholi Jr., "Harvard Dropouts: Some Psychiatric Findings," *American Journal of Psychiatry* 124, no. 5 (1967), 105. (The Unabomber was a Harvard graduate.)

- we have limited abilities for prophylaxis and treatment for many pathogens (the demand after an aerosol biological attack will be orders of magnitude beyond the level normally dealt with by metropolitan health systems[37]), and
- even if sufficient staff, equipment, and beds were available, for some pathogens we would be able to do little more than stabilize patients.

Commendably, we are building programs by generating responses to each of these perceived problems. Thus, we have: developed methods for inhibiting the spread of sensitive technologies (as for example, by passing laws requiring registration of certain pathogens and those who work with them[38] and by establishing a Federal advisory board on publication of potentially dangerous information[39]); experimented with building and other physical protection technologies;[40] established some detection capabilities;[41] expanded the numbers of our intelligence analysts expert in biology; and appropriated funds and created new authorities to encourage emergency hospital augmentation, drug development and government stockpiling of vaccines and pharmaceuticals.

Our programmatic approach suffers, however, from its compartmentalization of individual problems and its failure to recognize and come to grips with overarching issues that are likely to arise as terrorists escalate to biological weapons. In part, the challenge is to generalize so that we generate more comprehensive strategies, in part it is to think more deeply so that we see issues and opportunities that now elude us. These two attributes are linked. Broader strategies will be more robust and more penetrating.

Three Strategic Problems

To demonstrate this point, succeeding sections describe three overarching issues arising from biological weapons' special abilities to achieve *reload*, *comprehensive catastrophe*, and *surprise*. In each section

---

[37] I have expanded on this point in Richard Danzig, Rachel Kleinfeld, and Philipp C. Bleek, *After an Attack: Preparing Citizens for Bioterrorism* (Washington, DC: Center for a New American Security, 2007), available at <http://www.cnas.org/en/cms/?141>. See particularly 18–21 and the appendix.

[38] These regulations were authorized in the Bioterrorism Preparedness Act (2002).

[39] A major stimulus of this 25-member Department of Health and Human Services–sponsored National Science Advisory Board for Biosecurity was the Fink Report of the National Research Council, *Biotechnology Research in an Age of Terrorism* (Washington, DC: National Academies Press, 2004).

[40] In January 2002, the Office of Homeland Security established a working group on this subject. DARPA's Special Projects Office also established an Immune Building Program, and the Sloan Foundation actively funded projects focused on this area. A Sloan-funded effort of particular interest is a working group assembled by the Center for Biosecurity of the University of Pittsburgh Medical Center, on the use of HVAC systems to reduce risks from biological attacks. Penny J. Hitchcock, et al., "Improving Performance of HVAC Systems to Reduce Exposure to Aerosolized Infectious Agents in Buildings; Recommendations to Reduce Risks Posed by Biological Attacks," *Biosecurity and Bioterrorism* 4, no. 1 (March 2006), 41–54.

See generally National Institute of Occupational Health and Safety, "Guidance for Protecting Building Environments from Airborne Chemical, Biological or Radiological Attacks," available at <http://www.cdc.gov/niosh/docs/2003-136/2003-136b.html>, and "Guidance for Filtration and Air-Cleaning Systems to Protect Building Environments," available at <http://www.cdc.gov/niosh/docs/2003-136/> and the bibliographies in these documents. M. Ward et al. "The Effectiveness of Stand Alone Air Cleaners for Shelter-in-Place," *Indoor Air* 15, no. 2 (2005) 127–134, while urging additional analysis, conclude a technical study with the judgment that, "[s]teady-state concentration reductions of approximately 50% with a single air cleaner and more than 90% for three or more air cleaners are possible in residential dwellings,"133.

[41] A useful recent review of the large literature on the subject is National Research Council, *Sensor Systems for Biological Agent Attacks: Protecting Buildings and Military Bases* (Washington, DC: National Academies Press, 2005).

I will suggest examples of how our programmatic priorities will change if these characteristics are well understood and addressed.

Three observations may help in the evaluation of the discussion that is to come. First, these characteristics are not inevitably associated with bioterrorism. We can have, and should expect to have, instances of bioterrorism that do not involve reload, are not comprehensively catastrophic, and are not surprising. But my contention is that these characteristics are so important and likely eventually to manifest themselves that a sound, long-term strategy must address them.

Second, this paper is not comprehensive. Even fully addressing the three characteristics will only yield components of a strategy, not a comprehensive strategy. But the proposed method, if embraced, can point the way toward a strategy and identify an improved way of thinking about the long-term risk of bioterrorism.

Third, these three characteristics can be associated with other forms of terrorism. In my judgment they are most intensely prevalent in catastrophic bioterrorism (a term that will be defined below), and bioterrorism is the most important[42] and most challenging case for developing a risk-management approach. But because there is some commonality with other forms of terrorism, this paper may be useful as a model for thinking about other risks.

[42] A Central Intelligence Agency overview of terrorist risks concluded: "Our greatest concern is that [terrorist groups] might acquire biological agents, or less likely, a nuclear device, either of which could cause mass casualties**…** Terrorist use of biological agents is therefore likely, and the range of options will grow"CIA, "Mapping the Global Future: Report of the National Intelligence Council's 2020 Project," (Washington, DC: Government Printing Office, December 2004), 1, 3, available at <www.foia.cia.gov/2020/2020.pdf>.

CHAPTER FOUR

Reload and Interdiction

Terrorism, once predominantly a method of sporadic attack to call attention to a person or a cause, often is now used repetitively as a weapon of attrition. We have moved from incidents intended to terrorize to *campaign terrorism*.[43] The connection has not yet been forged between this strategic change and bioterrorism as an instrument. However, there is a great consonance between the two. Each is likely to feed the other.

The most fundamental, but remarkably little discussed, fact about bioterrorism is that it is not just about terrorists acquiring a pathogen and weaponizing it. Rather, this form of terrorism is likely to present itself in a more ominous form: terrorists acquiring a production capability. A terrorist group might acquire a nuclear weapon, but it is unlikely to acquire the ability to produce scores of them. Similarly, it is difficult for terrorists to produce a continuous campaign of World Trade Center–like attacks or other spectacular events. These attacks exhaust scarce resources (for example, hijackers who can fly airplanes), and they depend on surprise; once alerted, we have defenses (for example, strengthened cockpit doors, airport security, and combat air patrol) that make repeat attacks much more difficult.

Unfortunately, we do not have a significant ability to thwart repeated biological attacks. Furthermore, prevalent biological skills and equipment make it quite feasible to produce enough weaponized pathogens for repeated attack. Developing a pathogen as a weapon ("weaponization") is not simple. A virulent strain must be obtained, maintained, amplified, and embedded in a medium suitable for storage and dissemination without killing or disabling would-be attackers and without attracting the attention of police and intelligence agencies. But these challenges can be met in low-visibility laboratory and commercial environments. They require little more than broadly available skills and trial and error, supported by funding in the tens of thousands of dollars for simpler activities, or perhaps hundreds of thousands of dollars for more ambitious efforts.[44]

[43] This perception has been encouraged by Bruce Hoffman and Peter Chalk at the RAND Corporation and Brad Roberts at the Institute for Defense Analysis.

[44] As a point of comparison, "[T]he 9/11 plotters eventually spent somewhere between $400,000 and $500,000 to plan and conduct their attack." *The 9/11 Commission Report,* 169.

Once a small-scale capability is established to produce, for example, grams of anthrax, expanding that capacity to produce hundreds of grams or a few kilos is a comparatively modest hurdle.[45] Hundreds of grams would enable a terrorist to attack repeatedly. In the most severe form, he can do this by using aerosols (taking advantage of readily available technologies and devices) in our cities. Alternatively, large-scale bioterrorism can be perpetrated by infecting food and drink or by attacking livestock and crops. An attacker can be expected to take advantage of the small quantities[46] of pathogens that are required, their portability, their virtual invisibility, the time lag before symptoms resulting from an attack are manifest,[47] and the ease with which pathogens can be disseminated in any of many places and at considerable distances (particularly if an aerosol is used) from areas they will affect.[48]

However traumatic 9/11 was, or the explosion of a nuclear weapon would be, they are episodes. Like the attack on Pearl Harbor, when they are over, they are over. Attackers could not readily replicate their achievement. A biological attacker with a reload capability, by contrast, can mount a campaign by disseminating an aerosol in one city, then moving to another and another and another, and possibly returning to previous venues at will. Repeated attacks will complicate, and in many circumstances, vitiate our recovery plans. Moreover, an attacker with this advantage can hold us hostage.

An American strategy that recognizes reload must emphasize priorities that our present approach undervalues or ignores. *The most fundamental requirement is that we develop technologies and a concomitant concept of operations that give us the capability to interdict repeat attackers.* It is well and good

---

[45] In a paper for DARPA's Defense Sciences Office, I described two production alternatives, using anthrax as an example. The first of these, a "gram production capability," "would use standard laboratory equipment, costing tens of thousands of dollars, to produce grams (or liters) of agent in each batch. Once a seed agent was developed … such a system … could reach efficiencies where a ten or twenty liter fermenter (a level now unregulated by the Australia group) could produce ten or more grams of agent over the course of a week. By multiplying sets of equipment and running processes in parallel, production of scores of grams per week could be achieved. If an attacker was patient, willing to run the risk of discovery, and able to sustain the virulence of his product over the course of a year it would be possible to accumulate several kilos." A second route, a "kilo production capability" would have "at least two orders of magnitude greater capacity. It would require more mechanical skills, capital in the hundreds of thousands of dollars, surreptitious (but not terribly difficult) acquisition of equipment (probably on the used equipment market), and operations in rooms that would be more visible than bench top efforts. These operations would still be low visibility but would require a greater effort at disguise, perhaps as legitimate pharmaceutical or agricultural or brewery work. Utilizing larger fermenters and other apparatus, and probably engaging more than one person, these more substantial systems could produce several kilos of agent per month. Attackers who used the first system would have a reload capability only if they attacked with relatively small, but still quite potent quantities. (Recollect that the anthrax letters each contained only about a gram of agent.) Attackers who used the second system would have a reload capacity even if they used more than a kilo in each attack." Richard Danzig, *Reload and Its Implications* (paper for DARPA Defense Sciences Office, January 2005, fn. 5.) See also, Dana Shea and Frank Gottron, "Small Scale Terrorist Attacks Using Chemical and Biological Agents: An Assessment Framework and Preliminary Comparisons," (Washington, DC: Library of Congress, Congressional Research Service Report, May 2004). Since these comments were written, dry agar propagation has become increasing prevalent as an alternative method of obtaining spores.

[46] That is, by weight. Only about a gram of anthrax was reported to be in each of the letters mailed in 2001. But each gram was also reported to contain one trillion spores. Eight to 10,000 *b. Anthracis s*pores are estimated to constitute a lethal dose if inhaled by an average person. Thus, in theory, a gram perfectly and effectively and efficiently distributed and inhaled by an unprotected population could kill 100,000 people. In practice, I have suggested, "a reasonable approximate planning premise is that a gram of anthrax released in an urban area might expose between 100 and 1,000 people to a lethal dose. A kilogram (containing 1,000 trillion spores) could be anticipated to infect tens of thousands of people." Richard Danzig, *Catastrophic Bioterrorism: What is To Be Done?* (Washington, DC: Center for Technology and National Security Policy, 2003), 3.

[47] This period may range from minutes or hours (for biotoxins), to days (for pathogens such as *b. Anthracis*), to years (if, for example, prions—abnormally folded protein molecules that replicate in hosts—could be harnessed for attack).

[48] Weather conditions complicate outdoor aerosol attacks, making them unreliable for many military situations. Winds may carry them off target or even back upon friendly forces, rain makes attack impractical, and ultra-violet light degrades agents. But these problems are not disabling for a terrorist, who may be patient about timing and will accept devastation without precision.

to invest in intelligence and forensics, detection,[49] first responder capabilities, drug development, and consequence management—all priorities in our present program against bioterrorism. But, after a first attack, which of these programs will help us to interdict an attacker and prevent a second attack and then attack after attack after that?[50] Remarkably, this most essential question is now largely ignored. Our policing agencies are not merely uncommunicative about this point, they are unprepared. Our broader response resolutely ignores the problems of reload. Thus, for example, while our "national response plan" recognizes the possibility of multiple biological attacks and trumpets a requirement for "a non-traditional incident management approach," it circumvents the reload problem by assuming that these attacks will occur "simultaneously." It never mentions the risk of sequential, continued attacks. The "plan" recites:

> A biological incident may be distributed across multiple jurisdictions simultaneously, requiring a non-traditional incident management approach. This approach could require the simultaneous management of multiple "incident sites" ….[51]

Certainly, the problem of thwarting sequential attacks is difficult. But a sound strategy—especially an operational concept for coping with a long-term risk—cannot set priorities by concentrating on tasks that are most familiar (replicating efforts in parallel across several jurisdictions) or most rewarding to claimant constituencies (for example, spending on first responders and our public health system). Instead, we must recognize (why should this be surprising?) that our weaknesses are where our skills and constituencies are least robust. We must give priority to these areas.[52]

Recognition of the need for interdiction derives directly from an appreciation of reload and of the risks of comprehensive catastrophe. As I suggested in a previous essay,[53] there are four basic bioterrorist attack scenarios against which we must develop capabilities:

- an urban attack with an aerosol anthrax,
- dispersion of contagious pathogens,
- poisoning of food supplies with a toxin, and
- attacks upon our livestock, for example with foot and mouth disease.

Even if we successfully manage the consequences of individual attacks, repeated attacks through any of these modalities will wear down our response capabilities, our morale, and (as areas attempt to protect themselves and compete for resources) our national unity.

Technologies and operational concepts can be identified that will help us with interdiction. The appendix reproduces an article in which I suggest one approach to the premier problem of a large, outdoor, aerosol attack. This approach would use automated Laser Imaging Detection and Ranging

---

[49] Present approaches are well summarized in Daniel Lim et al., "Current and Developing Technologies for Monitoring Agents of Bioterrorism and Biowarfare," *Clinical Microbiology Reviews* 18, no. 4 (October 2005), 583–607.

[50] The "Beltway snipers" attacked 17 times in Maryland/Virginia in September–October 2003 before a tip led to their discovery asleep in their car. The Unabomber attacked 16 times 1978 to 1995 before he was turned in by his brother. A series of anthrax letters were mailed in the fall of 2001 before the attacker, unimpeded, stopped, apparently of his own volition.

[51] *National Response Plan* (Washington, DC: Department of Homeland Security, 2004, updated 2006), BIO-3, available at <http://www.dhs.gov/xlibrary/assets/NRP_FullText.pdf>.

[52] Our democratic system allocates resources to those who are most strongly represented. Our security requirements demand attention to our weakest constituencies.

[53] Danzig, *Catastrophic Bioterrorism: What is to Be Done?*.

(lidar) devices to detect and map manmade aerosol clouds as they develop over cities, pinpointing the source of a significant aerosol, and enabling police to recognize an attack as it develops and respond quickly enough to potentially capture an attacker. The concept may or may not work.[54] First analyses and tests of this approach suggest that it is worth further evaluation.[55]

The central point does not, however, pivot on the particular technology. Alternative methods can be devised to meet the challenge of locating the source of an aerosol in real time, and equivalent approaches can be developed for the other cases. But to do this, we must look the problem square in the face, direct and incentivize our laboratory and industrial base to address it, animate our policing agencies to plan for reload, and stop confining exercises and evaluations on an incident or simultaneous incidents that conveniently end and enable decisionmakers to turn to consequence management unimpeded by further attacks.

With respect to biological attack we are in a position similar to that of Britain in the 1930s, when it confronted the long-range bomber. The bomber—a terror weapon—initially was deemed unstoppable. Indeed, it *was* unstoppable in 1935, when that realization led the British to mount a research and development program to achieve the means to detect and locate aircraft and vector fighters to intercept them. That program produced an effective national air defense system within five years—just in time for the Battle of Britain.[56]

We need, urgently, to find a solution to our vulnerability. My proposal is merely an example of a line of thought. If it is correct, we will be stronger. If it is not, it is all the more important that we start investing as the problem demands, not according to our tastes and familiar preferences. Viewed correctly, interdiction is a policing problem, but it is too important to be left to traditional policing.

---

[54] The principal challenge is to discriminate between the signal given by attack aerosols and the noise of the background urban environment containing benign plumes (for example, from fires and construction) without so substantial a false positive rate (false alarms) as to call the system into question. Appendix A briefly describes this challenge, some related issues, and my reasons for believing that we can resolve them.

Note that this proposal differs from video surveillance in that the aim is not to deter attack or to capture an image of the attacker. Instead it is to geo-locate the point of attack (or, if the attacker is mobile, the line of attack) and to exploit the fact that catastrophic aerosol bioattacks, unlike crimes or attacks with explosives, are likely to be prolonged, making a terrorist vulnerable to arrest while in the act. On the pluses and minuses of video camera and other detection strategies with regard to crime or explosive devices see Martin Gill and Angela Spriggs, "Assessing the Impact of CCTV," Home Office Research Study 292 (2005), available at <www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf>, and Edward Kaplan, "Operational Effectiveness of Suicide-Bomber-Detector Schemes: A Best-Case Analysis," *Proceedings of the National Academy of Sciences* 29 (2005), 10399.

[55] For a discussion of the potential of lidars to complement current biological point detection systems see Shane D. Mayor, Paul Benda, Christina E. Murata, and Richard J. Danzig, "Lidars: A Key Component of Urban Biodefense," *Biosecurity and Bioterrorism* 6, no. 1 (March 2008), 45–56. A demonstration at the Pentagon is described in Thomas Warner et al., "The Pentagon Shield Field Program: Towards Critical Infrastructure Protection," *Bulletin of the American Meteorological Society* 88, no.2 (February 2007), 167–176. See also the description of the capabilities of a Ramon Eye-safe Atmospheric Lidar (REAL) in Scott M. Spuler and Shane D. Mayor, "Scanning Eye-Safe Elastic Backscatter Lidar at 1.54 Microns," *Journal of Atmospheric and Oceanic Technology* 22, no. 6 (June 2005), 696 ff and, more specifically, Shane D. Mayor, Scott M. Spuler, and Bruce M. Morley, "Scanning Eye-Safe Depolarization Lidar at 1.54 Microns and Potential Usefulness in Bioaerosol Plume Detection" (paper presented at SPIE Symposium on Optics and Photonics, August 2005).

[56] The term *radar*—for *ra*dio *d*etection *a*nd *r*anging—was coined by U.S. Navy officers in 1940, but the concept of using electromagnetic waves to detect large objects (ships and icebergs) dates to 1904, and the basic technology for detecting aircraft had been developed in the early 1930s by several nations, including Germany. The British were the first to develop and deploy a national system capable of directing fighter aircraft to intercept bombers. Great Britain and the United States retained an advantage in the operational applications of radar throughout the war. See generally Louis Brown, *A Radar History of World War II: Technical and Military Imperatives* (Bristol and Philadelphia: Institute of Physics Publishing, 1999) and, on British development and early defensive use of radar, Guy Hartcup, *The Effect of Science on the Second World War* (New York: St. Martin's Press, 2000), 18–59.

CHAPTER FIVE

Comprehensive Catastrophe, Public Preparedness, and Natural Pandemics

Comprehensive Catastrophe

We commonly invoke our most extreme language when we encounter very large events; we call them "catastrophic." But our thinking and our language need to distinguish between two types of catastrophe. First are those events that cause hundreds or even thousands of deaths or injuries, but are dealt with by waves of reinforcement from outside the affected areas. These might be described as *contained catastrophes*. Victims are told to hold on because "the cavalry is coming," as the Mayor of New Orleans repeatedly said he expected in the wake of Hurricane Katrina. Beyond this type of catastrophe lies another, fortunately rare. I will call this type *comprehensive catastrophe*.[57] A comprehensive catastrophe is so extensive that it does not permit one jurisdiction to aid another. In this case, one or more of the following conditions exist:

- so many jurisdictions are victimized that they are unable to provide resources to one another,
- jurisdictions are afraid they will be victimized, and so they horde resources,
- basic services (particularly fuel, communications and transportation) are so overwhelmed that near-term, external assistance cannot be provided,
- movement restrictions and transportation system failures prevent rapid external assistance.

For any or all of these reasons, in a comprehensive catastrophe each jurisdiction, group, or family must rely predominantly on its own resources.

[57] Note that traditional definitions of disaster conflate the two conditions that I am distinguishing. Thus, see for example, Kathleen Tierney et al., *Facing the Unexpected: Disaster Preparedness and Response in the United States* (Washington, DC: National Academies Press, 2001), 8, endorsing the definition of disaster advanced by C.E. Fritz in 1961: "An event, concentrated in time and space, in which a society, or a relatively self-sufficient subdivision of a society, undergoes severe danger and incurs such losses to its members and physical appurtenances that the social structure is disrupted and the fulfillment of all or some of the essential functions of society is prevented."

Comprehensive catastrophes go beyond inflicting great injury; they call into question our near-term abilities to recover.[58] Of the instruments available to terrorists, only bioterrorism and nuclear terrorism are likely to reach this level.[59]

Bioterrorism can certainly present itself in attacks that cause small and intermediate damage. In the brief history of bioterrorism in America, we have experienced only small-scale incidents: a salad bar salmonella contamination,[60] ricin poisonings,[61] and distribution of single grams of anthrax through the mail. These events, though injurious, are like familiar forms of terrorism—the Unabomber's pipe bombs or, on a more massive scale, the Oklahoma City bombing and 9/11. Though terrible for their victims and terrorizing for others, we are able to respond to these attacks within the capabilities of existing systems. They do not challenge either our government or our abilities as private citizens to pursue our chosen courses of action. After the trauma of these incidents, though our society may be scarred, it continues essentially as it was before. In the days after these events, other priorities reassert themselves: people go to work, travel resumes, and our financial markets, if they were closed, reopen. However tragic for those most directly affected, for the nation as a whole these attacks are more like drive-away accidents than head-on collisions. They jolt us and can cause real injury, but they do not disable us or divert our society from its normal patterns.

Some quite plausible acts of bioterrorism will, by contrast, cause comprehensive catastrophe. In the areas where they occur, these attacks will provoke orders-of-magnitude increases in demands for support, health care, and advice at the same time that they disable our restorative systems (for example, transportation, communication, and hospital care) and induce disruptive citizen behaviors (for example, flight, violence, and demands for service by large numbers of "worried well").[62] They will also affect behaviors in areas where they do not occur, as a result, for example, of fear and the urge to hoard. Not all attacks will have these effects. But some—for example, repeated,[63] urban, aerosol attacks using anthrax—pose the most fundamental challenges to the capabilities and the character of our country and therefore must be addressed.

If we appreciate this risk, we cannot build our strategies exclusively around incremental expansion of existing systems, for example, by expecting to manage health consequences by bringing

---

[58] Some would argue that these attacks will be existential, that is, they may challenge our abilities to ever recover. I believe that we are resilient enough to meet these challenges over the longer term, as seventeenth-century societies did in the face of comprehensively catastrophic plagues. I believe, though, that we must recognize that our cooperative relief mechanisms will be much less than normally effective in the weeks and months immediately after comprehensive catastrophes.

[59] A campaign using explosive devices could reach this level if it were widespread and sustained, for example, the Palestinian campaign against Israel at the turn of the century. It seems unlikely, however, that such a campaign can be initiated and maintained in America in the foreseeable future, given both the attitudes of this population and the absence of an adjacent base in which terrorists can find sanctuary and from which they can readily pass into America without recognition.

[60] Seven hundred and fifty-one cases of food poisoning resulted, but there were no deaths. T.J. Torok et al, "A Large Community Outbreak of Salmonellosis Caused by Internal Contamination of Restaurant Salad Bars," *Journal of the American Medical Association* 278, no. 5 (August 6, 1997), 389–95. See also Miller, Engelberg, and Broad, *Germs,* 15ff.

[61] There are ample foreign precedents. In 1978, Bulgarian dissident Georgi Markov was killed by a tiny, ricin-filled pellet injected into his leg while he was walking on a London street. See <http://news.bbc.co.uk/1/hi/uk/2636459.stm>. From1981 to 1995, "Project Coast," a South African program researching chemical and bioterror weapons was focused on agents "intended to be used for assassination and crowd control…," Chandre Gould and Peter Folb, *Project Coast: Apartheid's Chemical and Biological Warfare Programme* (Geneva: United Nations Institute for Disarmament Research, 2002), 2, and see 159–168 for a catalog of "incidents of poisoning" associated with the program.

[62] New Orleans' experience with Hurricane Katrina, which occurred after this section was written, displayed some of these effects, but even in that horrific context, the experience was confined to a region, leaving the rest of the country free to provide support and to attend to its other priorities with only near-term impacts of higher prices.

[63] I.e., those that take advantage of reload.

hospital staff and beds from other areas. Particularly when coupled with reload and surprise (the latter described below), they demand a different kind of systemic planning.

Public Preparedness[64]

Our biodefense program is planned and executed by professionals. Hospital physicians, nurses and administrators, public health officials, infectious disease experts, police, fire, and other "first responders," emergency preparedness experts, military officers, biologists, physicists, chemists, and environmental analysts, among others, all power our efforts to prepare for potential catastrophe. Their indispensable and admirable professionalism has rich rewards. But it also creates great problems. In previous work, I have emphasized one of these problems: the difficulty of combining conceptual domains so that diverse perspectives, vocabularies, and tools can be harnessed to produce a comprehensive strategy.[65] The requirements of a long-term strategy suggest another, no less significant, weakness of our present professionalism.

Our consequence management preparations are so focused on professional command and control with the goal of optimized care for each case (the hallmarks of good responses to smaller, better controlled, and better predicted events) that we largely overlook the need to create a supplementary lay system that can sustain and empower people caring for themselves and one another without traditional professional support.[66] Yet, comprehensive catastrophe and reload can overwhelm our professional systems. They therefore make the supplementary system imperative.

In this requirement, moreover, lies opportunity. The two systems together will be more robust and resilient (i.e., they will be less likely to fail)[67] than either would be alone. Furthermore, the

---

[64] I turned to this topic again with the assistance of co-authors in *After an Attack*. Interested readers will find both an expanded discussion of the points in this section and, in section III, a set of recommendations that may improve our position in this regard.

[65] Danzig, *Catastrophic Bioterrorism: What is To Be Done.* As noted in Part I, this problem considerably contributes to our difficulties in evolving a long-term strategy to counter the risk of bioterrorism.

[66] A substantial literature examines aspects of the problem but has not coalesced into an analysis that animates decisionmakers or provides a program outline that is likely to be adopted. This discussion benefits from that literature while attempting to move beyond it. Particularly notable previous contributions address expected or desired public behaviors and recommended government behaviors. Among those predominantly focused on public behaviors are Clete DiGiovanni et al., *A Prospective Study of the Reactions of Residents of an American Community to a Bioterrorist Attack* (Bethesda, MD: Defense Threat Reduction Agency, 2002) (presenting Louisiana citizens with an extended video about a hypothetical intentional West Nile Disease outbreak and evaluating their reactions as reflected in questionnaires); and Lynn Davis et al., *Individual Preparedness and Response to Chemical, Radiological, Nuclear and Biological Terrorist Attacks* (Santa Monica: RAND, 2002). Predominantly focused on recommending governmental behaviors are: The Working Group on "Governance Dilemmas" in Bioterrorism Response, "Leading During Bioattacks and Epidemics with the Public's Trust and Help," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 2, 1, (2004), 25–40, available at <http://www.liebertonline.com/doi/abs/10.1089/153871304322964318?journalCode=bsp>. Blending the two approaches in particularly useful overviews are Bradley D. Stein et al., "Emotional and Behavioral Consequences of Bioterrorism: Planning a Public Health Response," *The Milbank Quarterly* 82, no. 3 (2004), 413, and Thomas Glass and Monica Schoch-Spana, "Bioterrorism and the People: How to Vaccinate a City Against Panic," *Clinical Infectious Diseases* 34, no. 2 (2002), 217–223, and ed. Nancy Ethiel, *Terrorism: Informing the Public* (Chicago: McCormick Tribune Foundation, 2002). See also a classic work by the National Research Council Committee on Risk Perception and Communication, *Improving Risk Communication* (Washington, DC: National Academy, 1989).

[67] Our present response model is analogous to that of a mainframe computer: programmed, built around a central processing unit, vulnerable to errors in input, and ill-equipped to adapt to deviations. What we need is a system that operates more like the human brain—decentralized, flexible in the face of error and surprise, capable of rapid learning, and tolerant of failure. The distinction between the two systems is well made by Jeff Hawkins and Sandra Blakeslee, *On Intelligence: How a New Understanding of the Brain Will Lead to the Creation of Truly Intelligent Machines*, (New York: Times Books, 2004), 12.

supplementary lay system will address political and psychological needs now largely neglected, but central to the battle between terrorists and our government.

The neglect of laymen is understandable. We live in a society that idealizes and relies upon professional competence. We employ licenses (predicated on training), rewards (dollars and prestige), and punishments (e.g. by a ban on unauthorized practice of medicine) to reinforce the division of labor. By these means, also, we seek to assure consistency and quality in professional services. Conversely, we distrust laymen. Their ethics, skills, knowledge, and judgment vary widely. One well-designed survey of laymen flatly concluded: "The majority of respondents have a number of beliefs about smallpox and smallpox vaccination that are false."[68] Deficiencies run deeper than this. In an urban area beset by biological crisis, we can anticipate that a third of all citizens are likely to be depressed, alcoholic, addicted, paranoid, psychotic, incarcerated, elderly,[69] infirm, disabled,[70] infants and children,[71] immature adolescents,[72] or some combination of these. Moreover, a quarter of the populations of New York and Los Angeles, for example, describe themselves as not speaking English "very well."[73]

Need to Rely on Laymen

In this light, how can anyone argue that our mode of response should more heavily rely on the response of civilians? There are, however, four compelling reasons why that must—and should—be so.

First, our existing models will not work: professionals cannot alone cope with comprehensive catastrophic bioterrorism. Everyday economic pressures have eradicated excess professional capacity. The spare capacity that can cope with comprehensive catastrophe is not in our professional systems. Surge capabilities are predominantly located in our citizens because in an emergency they will put aside everyday tasks and care for their families, their friends, and themselves.

Second, citizen behaviors will greatly increase or diminish the effects of an attack and the workload of our professionals. Evacuation, health care, security, decontamination, and other activities are

---

[68] Robert Blendon et al., "The Public and the Smallpox Threat," *New England Journal of Medicine* 348, no. 5 (December 19, 2002), 426–432.

[69] One out of every eight Americans (that is, 35 million people) is over the age of 65. U.S. Census Bureau, Census 2000, Table DP-1, Profile of General Demographic Characteristics for the United States: 2000.

[70] One in every twelve Americans (that is, 18.2 million people) aged 16 or older has a condition that makes it difficult to go outside the home to shop or visit a doctor. Judith Walrop and Sharon M. Stern, U.S. Census Bureau, Census 2000 Brief, Disability Status 2000. Ten percent of the population of New York City between the ages of 5 and 21, and 25 percent of the population between the ages of 21 and 64 are reported in the 2000 census as disabled. U.S. Census Bureau, 2000 Census, DP-2. Profile of Selected Social Characteristics: 2000, Census 2000 Summary File (SF 3)— Sample Data.

[71] Of the 281.4 million Americans enumerated in the 2000 census, 6.8 percent (19.2 million people) were under the age of 5, and 7.3 percent (20.5 million people) were between the ages of 5 and 9. U.S. Census Bureau, Census 2000, Table DP-1, Profile of General Demographic Characteristics for the United States: 2000.

[72] Seven and three-tenths percent of those enumerated in the 2000 census were between the ages of 10 and 14. U.S. Census Bureau, Census 2000, Table DP-1, Profile of General Demographic Characteristics for the United States: 2000.

[73] Of the 7.5 million New Yorkers over the age of 5 enumerated by the 2000 census, nearly 1.8 million (23.67 percent) described themselves this way. U.S. Census Bureau, Census 2000 Summary File 3, Profile of Selected Social Characteristics, District of Columbia. Of 8.8 million people enumerated in Los Angeles County, over 2.5 million (28.9 percent of the total population) described themselves this way. Ibid, Profile of Selected Social Characteristics, Los Angeles County. It is hard to discern how many of these people have a functional grasp of English. On a national basis, the census recorded 8.1 percent (21.3 million people) of the total population as not speaking English "very well," but half of these described themselves as falling in the next best category—they judged that they spoke English "well." The other half described themselves as speaking English "not well" (7.6 million people) or "not at all" (3.4 million people). U.S. Census Bureau, Census 2000, Summary File 3, Tables P19, PCT13, and PCT14.

much more burdensome or notably easier, depending on the conduct of the laymen involved.[74] While we are struggling to expand the supply of professionals, we are overlooking large rewards from approaching this problem at the opposite end—by reducing citizen demand.

Supplementary lay system is essential because

- **Professionals alone cannot cope with catastrophe**
- **Appropriate behavior of citizens will reduce demand**
- **Prepared citizenry will be more cohesive**
- **Informed citizens will support dedication of resources**

Third, a terrorist attack on us aims to affect the minds, even more than the physical well-being of our citizens. It is through their reactions that the effects of terror are amplified or eviscerated. A much-quoted insight of Clausewitz is as applicable to terrorism as to conventional conflicts. Each "is a trial of moral and physical forces through the medium of the latter … psychological forces exert a decisive influence on the elements involved in war."[75] A catastrophic attack will be a psychological and a political intensifier: it will either increase our national unity and support of our government or, as terrorists intend, it will induce divisiveness, loss of confidence, and distraction.[76] Our prospects in either direction are greatly affected by whether our government has prepared citizens and can effectively communicate with and support them at a time of trauma.

Finally, in a democracy public awareness and engagement before an attack will affect public support for programs that are intended to counter the effects of potential attacks. If laymen are indifferent and disengaged, professional programs will tend to sink, as they have, into a morass of interest-group politics with too little attention to the larger public interest. A bioterrorism working group concerned with this problem observed that leadership with respect to epidemics:

> entails consciously pursuing and institutionalizing a sense of shared responsibility for the public's health—among leaders, between leaders and the public, and among community members themselves. Principles for achieving this sense of shared responsibility include approaching the public as a capable ally, not as a problem that needs managing …[77]

The first two of these four points may demand some further explanation.

Regarding the first—the inability of professionals alone to cope with comprehensive catastrophe—the surge capacity is in our citizens. The 5,000 hospitals in the United States have limited surge capacity, because market pressures have wrung extra beds, personnel, and facilities out of the system.

---

[74] In fact, they often depend on the responsiveness of laymen. Clete DiGiovanni et al., "Factors Influencing Compliance with Quarantine in Toronto During the 2003 SARS Outbreak," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 2, no. 4 (2004), 265–272: "… the public health authorities often relied on members of the general public to report themselves to quarantine hotlines if they met the criteria announced in public service messages …," 267.

[75] Karl von Clausewitz, *On The Theory of War* (Princeton: Princeton University Press, 1984), 127.

[76] This has practical as well as psychological and political consequences. A working group that reflected on this problem reported: "Some employees of American Media, Inc.—the site of the first anthrax case—were doubly victimized: Long-time physicians refused to care for them; schools turned away their children; those with 'second' jobs as housekeepers were not allowed into homes to clean. Recovered SARS patients, their families and neighbors, doctors and nurses, formerly quarantined contacts have been shunned globally." The Working Group on "Governance Dilemmas" in Bioterrorism Response, "Leading During Bioattacks and Epidemics with the Public's Trust and Help," 29.

[77] Ibid., 36.

A typical urban hospital operates with a daily patient census close to 100 percent of its intake capability.[78] (An ordinary citizen may experience this when, after an unexpected problem warranting admission, he or she is held in an emergency room until a bed becomes free. During flu season, it is common for hospitals to divert patients because of lack of space.) All facilities have emergency plans, and our Federal response is built around them. But these plans achieve only small gains by steps like deferring elective surgeries. Beyond steps of this kind, each hospital plans to cope by diverting patients to, and drawing reinforcement from, other facilities. Hospitals will quickly be overwhelmed if these supporting resources are not available because manpower and supplies are not released (as may well occur in a reload situation), exhausted (as is likely if a catastrophe is widespread), or disabled (as in instances of crippling catastrophe).

The system is afflicted with double- and triple-counting. Hospital security personnel are commonly off-duty policemen and national guardsmen subject to mobilization. Doctors have privileges at—hence, are on the rolls of—more than one hospital. Furthermore, when contagious illness is rampant, it is reasonable to expect that their own illnesses, fear, and family demands would reduce, not increase, the number of health professionals available for duty. John Barry's description of a military hospital in the influenza epidemic of 1918 ("… 70 out of 200 nurses were already sick in bed themselves, with more falling ill each hour")[79] could certainly apply in the wake of a 21st century biological attack. A survey in 2004 reported that a third of 385 clinical and non-clinical workers in an American suburban health care facility and level 1 Trauma Center stated that they expected that they would not come to work "if there were biologically exposed patients in the hospital."[80]

Regarding the second, there will be seven components of citizen demand on our health care system in the wake of a catastrophic attack: those who require hospital treatment for illness or injury related to the attack; those who require hospital treatment for illness or injury unrelated to the attack; those who suffer from a somatic problem warranting medical diagnosis to determine whether they fall into the first two categories; people who require or request preventive treatment (as for example, those who seek antibiotics because they may have been exposed to anthrax); the so-called "worried well" who do not have a somatic problem but believe otherwise, or are not sure and seek reassurances that they are not infected; those who require information and medicine to care for themselves or others at home; those seeking information about relatives and friends who are missing or being treated. Our planning attention has focused on the first three categories, but the last four are likely to be the more numerous.

---

[78] Suburban hospitals sometimes have more leeway. Their emergency response capabilities, however, are normally limited by the absence of round-the-clock laboratories, shortages of equipment (for example, ventilators), and shortages of staff (for example, infectious disease specialists). Danzig, Kleinfeld, and Bleek, *After an Attack* provides a detailed analysis of hospital bed and emergency room capacity in the National Capital Area, 41, 42.

[79] John M. Barry, *The Great Influenza: The Epic Story of the Greatest Plague in History* (New York: Penguin Group, 2004), 189.

[80] Dan Hanfling et al., "Will They Come To Work? Evaluating Healthcare Workforce Knowledge And Intent Regarding Hospital Disaster Response" (unpublished survey conducted in December, 2004): "When asked if they would report to the hospital to work, 32% (95% CI: 28–37%) reported that they would not do so if there were radiologically contaminated patients in the hospital, 27% (95% CI: 23–32%) would not report for work if there were chemically contaminated patients in the hospital, and 34% (95% CI: 30–39%) would not report for duty." On the other hand, DiGiovanni et al. report that "[a]lthough Killian, in a seminal paper published 50 years ago, raised the possibility that emergency personnel might abandon their jobs and tend, instead, to the needs of their families during a community disaster, Quarantelli investigated the response of over 6,000 emergency workers in 150 tornadoes, floods, hurricanes, and earthquakes between 1964 and 1974, and found no evidence that these workers abandoned their official responsibilities," 2.

Though references to the worried well abound, very little research, much less analysis, has been done on the topic.[81] It is clear, however, that the ambiguity of bioterrorist attacks will cause those events, once known, to produce requests (one may reasonably say, demands) for assessment and treatment that are a multiple of the cases in which individuals are actually infected. Thus, for example, after the Aum Shinrikyo cult attacked the Tokyo subway system in March, 1995, ten times as many people streamed into St. Luke's Hospital as were actually found to have been exposed to sarin.[82] Most members of this group were acting quite rationally; an attack had occurred, and they needed attention to determine if they were exposed. The boundaries of a mass biological attack (especially an outdoor aerosol attack) will not be subject to rapid assessment; such assessments as are likely eventually to be made will not be authoritative; even if authoritative, they will not be believed; and, even if believed, the fear of reload will lead substantial segments of the population to believe that they have been (or will be) exposed, quite apart from the facts of the situation. These psychological realities can only be dealt with by addressing the lay populations themselves.

In the wake of catastrophic attack, citizens will demand

- **treatment for illness or injury from attack,**
- **treatment for illness or injury unrelated to attack,**
- **diagnosis for somatic problem that could be either of the above,**
- **preventive treatment,**
- **medical advice out of concern,**
- **information and medicine for themselves or others at home,**
- **information about relatives and friends.**

A simpler problem is posed by those seeking information about family members and friends. Israeli and other experiences demonstrate that some logistical initiatives (for example, centralized and widely accessible patient registries) can combine with educating the affected populations about the use of these instruments to notably diminish hospital crowding and first responder distractions. In planning for crippling catastrophe, we need to inventory these mechanisms, establish relevant systems, and prepare the public to use them.

Toward an Effective Citizen Outreach Program

On first examination it appears that the public is like a large sea—it is too big a body for us either to animate when it is placid or contain when it is disturbed. Our citizens, confronted with a great number of everyday concerns and longer-term warnings, are not likely, en masse, to prepare for bioterrorism. On the other hand, when an event occurs, it will be difficult to communicate with them, win their trust, organize them, and be able to help. We also have some reason to distrust them—proposals, for example, to distribute supplies of antibiotics in advance inspire fears of loss, misuse,

---

[81] Decrying the absence of evidence, Stein et al. report that "the U.S. Department of Defense estimates that an attack from a CBRN weapon would produce five psychological casualties for every one physical casualty (Warwick 2001); other estimates of the ratio of psychological to physical casualties range from 4 to 1 to as high as 50 to 1. (Demartino 2002)," "Emotional and Behavioral Consequences of Bioterrorism: Planning a Public Health Response," 414.

[82] T. Okumura, "Report on 640 Victims of the Tokyo Subway Sarin Attack," *Annals of Emergency Medicine* 28, no. 2 (August 1996), 129–135.

and abuse. Conversely, many of our citizens distrust government. As described below, this group is worrisome in its size and intensity of conviction.

In three respects, though, we have opportunities to better support laymen.[83]

The first is to prepare messages and mechanisms that can be utilized in an emergency, i.e., when the public is engaged.[84]

A second would be to invest in technologies that can provide information without citizens going to the hospital or physically encountering doctors. Americans now routinely use websites like WebMD, Healthwise, and World Doc to obtain health information. They use telephones, cell phones, computers, and BlackBerry services to secure individualized feedback. None of these mechanisms existed when the Spanish Flu struck in 1918, and few of them have been relevant to any previous American epidemic. All may be overwhelmed in the short term by peak demand as news of a terrorist attack spreads.[85] There are risks of disruption from cyber attacks.[86] But it is reasonable to expect that these systems can be strengthened enough to endure and stabilize in the wake of a biological emergency.

Though emergency notification systems now use computer-generated cell phone calls[87] and the Internet, they essentially function as radio and television notices have in the past. We have not sufficiently invested in the opportunities presented by the proliferation of these new technologies among ordinary citizens.[88] Human response mechanisms will be erratic and overwhelmed in the face of catastrophe. Hospitals and public health departments have only a miniscule capacity to respond to

---

[83] These ideas are expanded upon in Danzig, Kleinfeld, and Bleek, *After an Attack*.

[84] In its response to SARS, "Singapore contrasted sharply with the anecdotal accounts of near-panic in some other countries, where it was reported that implementation of preventive measures was much delayed, communication was haphazardly done, and actions were uncoordinated, resulting in substantial human and economic cost…. Quah et al. found that more than 80% of Singaporeans thought that official information given on the SARS situation was 'accurate, clear, sufficient, timely and trustworthy.' The level of anxiety of the general population was found to be relatively low." David Koh et al., "Risk Perception and the Impact of Severe Acute Respiratory Syndrome (SARS) on Work and Personal Lives of Healthcare Workers in Singapore: What Can We Learn?," *Medical Care* 43, no. 7 (July 2005), 676, 682, citing S.R. Quah et al., "Crisis Prevention and Management During SARS," *Emerging Infectious Diseases* 10, no. 2 (February 2004), 364–368.

It is doubtful that we Americans will perform as well in a catastrophic bioterrorist situation. Some of the differences in performance relate to size and cultural diversity. But preparation is also insufficient. The Centers for Disease Control, the Department of Homeland Security, and other organizations have prepared templates identifying key questions that they need to address in the wake, for example, of an anthrax attack. Though a useful first step, these preparations do not go far enough. We should now have prepared answers to these questions based on the best achievable consensus of experts. It is correct to note that answers would depend on the facts of particular occurrences, but (a) a base-line set of responses would provide a basis for modification and (b) many facts will be unknown at the time messages are required (for example, it might take some time to know whether anthrax was antibiotic resistant). Messages should now be prepared (even if not yet published) providing advice, in the case of anthrax, for example, about self-decontamination, living and work quarter procedures, self and family treatment, and movement. Citizens will also need to be advised about the possibilities of reload.

[85] During the 9/11 attacks, "Attempted calls via Cingular Wireless increased 400 percent in Washington and 1000 percent in New York," *SMS over SS7,* National Communications System Technical Information Bulletin 03-2, December, 2003, as cited in Enck et al. NCS TIB 03-2 is available at <http://www.ncs.gov/library/tech_bulletins/2003/tib_03-2.pdf>.

[86] For a recent description emphasizing the cyber-terror risk to phone networks, see William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta, "Exploiting Open Functionality in SMS-Capable Cellular Networks," *Proceedings of the 12th ACM Conference on Computer and Communications Security* (November 2005).

[87] Cellphones have drawbacks for location-based notices. When a refinery fire broke out in California in 2007, state officials were only able to reach cellphone users who had registered their street addresses and phones, missing visitors and new residents. Zachary A. Goldfarb, "Emergency Alert System Uses Cellphones in Specific Areas," *Washington Post*, January 7, 2008, D01, available at <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/06/AR2008010601742.html>.

[88] A large market has developed for the sale of these systems to first responders. See, for example, Palm's August 2003 "White Paper: Using Wireless Technologies to Address Bioterrorism and Other National Threats" available at <http://industries.bnet.com/whitepaper.aspx?&tags=Handhelds&docid=145531> (registration required).

requests for advice. Under emergency conditions, face-to-face contact is likely to involve medical professionals and patients with no prior relationship, functioning in unstructured, unfamiliar, extremely rushed, poorly monitored, badly documented, and highly stressed environments. This is a recipe for harm and frustration.

In this context, automated systems warrant investment. With essentially unlimited capacity and stamina, "cyber-care" systems[89] can be designed to accept citizen calls through digital instruments, elicit keyed-in information (for example, about location, illness, or injury), provide first-order recommendations in response to this information, flag the most urgent cases, direct family members to one another, and compile an overall picture for decisionmakers.[90] These systems will be even more valuable if electronic medical records are established and maintained before a catastrophic incident.[91] Absent this effort, it can be expected that, as in New Orleans in the wake of Hurricane Katrina, health records will be inaccessible or destroyed.

Electronic systems do not dispense with the need for expert follow-up, but they facilitate expert work, and, when experts are unavailable, can be valuable mechanisms of support and comfort.[92] Moreover, they will diminish demands on overstressed hospitals. And beyond that, scarce and precious expert follow-up will be more appropriately dispensed if it is designed to take advantage of these first-level screens. (For example, a system of mobile nurses and facilities could be structured to visit neighborhoods, with information, supplies, and appointment times determined by the results of the first computerized communication.)

A third step would add a human dimension to these technological improvements. I believe that we should experiment with identifying and training organizational representatives from what a RAND research team called "natural support systems" (for example, workplaces, schools, and churches), where Americans gather and to which they customarily look for advice.

---

[89] Joseph Rosen, "Cybercare—A Strategy for Biodefense: Improving the Response of NDMS," unpublished briefing, Department of Defense, January 31, 2003.

[90] These systems take advantage of modern telecommunications and artificial intelligence to provide medical advice to caregivers and patients at remote locations. The common, underlying concept is that patient and doctor movement can be obviated and patients made more self-sufficient by utilizing computer information systems. For example, EMMI (<www.rightfield.net/whatisemmi.shtml>) walks U.S. patients through pre-surgical and surgical procedures, enhancing understanding and enriching the resulting informed consent. Virtual Health Care Coach (<http://virtualhealthcoach.com>) provides tailored coaching for withdrawing from substance abuse, exercising, etc. Teledoc operates in rural India (<www.jiva.com/health/teledoc_dev.asp>) to guide lay medical personnel in treatments.

A 922 system (comparable to the 911 phone number) has been proposed for the United States. In this system, a patient or family giver who called 922 would be prompted to press one number for a fever above a specified level, another for the age of the patient, etc. The system would then provide recorded advice, including whether to proceed to a hospital. (Compilation of data from calls would also permit some insight into the type and distribution of health problems, at least as self-reported.)

DOD operates a much more sophisticated system, involving assistance to shipboard doctors or medical corpsman by transmission of x-rays, etc. In a 2003 briefing, Dr. Joseph Rosen, a DOD Health Affairs consultant, suggested that a basic version of the system could be used in civilian health emergencies. Joseph Rosen, "Cybercare." See also, Christopher Swift et al., "Homeland Security and Virtual Reality: Building a Strategic Adaptive Response System (STARS)" in ed. J. D. Westwood et al., *Medicine Meets Virtual Reality: The Magical Next Becomes the Medical Now, Studies in Health Technology and Informatics* 111 (Amsterdam: IOS Press, 2005).

[91] Regular health care systems are moving in that direction. See generally Timothy J. Mullaney, "A Booster Shot for Medical Data-Sharing," *BusinessWeek* (November 10, 2005).

[92] "Nearly three out of four Americans (72 percent) say they favor the establishment of a nationwide electronic information exchange that would allow a patient's health information to be shared with authorized individuals quickly, privately, and securely via the Internet." Markel Foundation Press Release, "Americans Support Online Personal Health Records" (October 11, 2005), available at <www.markle.org/resources/press_center/press_releases/2005/press_release_10112005.php>.

> These natural supports are often not formally integrated into a community's disaster response plan, even though their importance in helping individuals deal with disasters and other traumatic events has been widely demonstrated …. Support systems also provide a natural avenue through which to educate the public as part of preparing for and responding to a bioterrorist event.[93]

Unfortunately, the concept remains undeveloped. At full scale, if one volunteer representative were identified for every one to two hundred people, a program of this kind might involve 500,000 to 1,000,000 "emergency representatives." Initially, though, we should test and develop this concept in a program a thousandth of this size—that is, an effort involving five hundred to a thousand representatives.

The concept resembles the World War II employment of volunteer block wardens.[94] Volunteers would receive a day of training about biological and other catastrophic risks, both natural and terrorist. Telephone and web access would be established to enable communication before, during, and after emergencies. More ambitiously, in a test case, emergency representatives could also be supplied with antibiotics and other equipment that would be maintained under their control but distributed when needed (including, if authorized, in the context of a natural epidemic, such as SARS or Avian Flu). At a minimum, this program would enlist emergency representatives to provide tailored and credible information for their coworkers or associates in a catchment area. Further, if connectivity could be maintained, these same emergency representatives could form a network that conveyed continuous information from centralized professionals to ordinary citizens, and from these citizens back to those attempting to manage the crisis.

A network of this kind would have psychological and practical benefits. Messages can be transmitted from central locations, but under conditions of uncertainty and urgency, these messages often are distrusted, misunderstood, misapplied, or not received.[95] Particularly when supported by senior, respected figures (for example, a minister, a supervisor, or a family doctor), peers are trusted and can provide better-crafted and more responsive information.

A New York Academy of Medicine study found that 41 percent of those questioned about their reactions to government messages in the wake of a hypothesized smallpox attack expected that the government would conceal or withhold information, lie, experiment on people, look after the interests of Caucasians at the expense of minorities, or all of the above. More than a quarter indicated that they would be afraid to go to a smallpox vaccination site.[96] These results cannot be ignored, dismissed as an artifact of the study design, or addressed simply through improved crafting of messages from authorities.

---

[93] Ibid., 443–444.

[94] "Defined as the 'backbone of civil defense,' block wardens assumed considerable responsibilities both in the neighborhood and the community at-large. Responsible for an average of 500 people, block wardens taught civil defense regulations, prepared a map of the neighborhood, kept an accurate census of the block, trained people how to fight fires and administer first-aid, distributed government literature, and remained in charge of preventing panic." See "Women Defend the Nation," available at <www.coldwar.org/articles/50s/women_civildefense.html>.

[95] Stein et al., "Emotional and Behavioral Consequences of Bioterrorism: Planning a Public Health Response."

[96] Roz D. Lasker, *Redefining Readiness: Terrorism Planning Through the Eyes of the Public* (New York: New York Academy of Medicine, 2004), findings of a conference sponsored by the New York Academy of Medicine and the Center for the Advancement of Collaborative Strategies in Health.

Social science research suggests that after a period of "numb dedication," victims of mass trauma move to a psychology of "anger-betrayal."[97] A gap between citizens and professionals will need to be bridged. A CDC Foundation conference about Toronto's experience with SARS observed that when government messages are echoed by trusted employers they gain credibility.[98] The conference report concluded:

> In an emergency, employees demonstrate an increased tendency to gravitate toward the familiar communications channels set up by their own employer, more so than during normal times. Similarly, employers increased the depth of their communications to their own employees on a wide sector of issues including:
>
> - confirming location and status of employees and their families
> - indicating when and if to report to work
> - encouraging proper personal protection and risk reduction messages
> - describing how to clean work areas and equipment
> - handling rumor control and stigmatizing incidents[99]

Beyond the business arena, it is clear that Federal, state, and local policies can build trust and facilitate citizen resilience, or they can erode these assets. A disabled person must manage his own participation in society, but government assists that participation by small steps, like designated subway seats and parking spaces, and by larger ones, like training programs and legislation prohibiting discrimination. In the same manner, the resilience of our citizens individually and en masse will largely be a consequence of their own qualities and circumstances, but, as with the disabled, individual commitments and successes can be very substantially affected by government policies and preparations. A little-noted draft legislative act seeks to force "public policies … to facilitate [citizen] resilience."[100]

It is critical not simply to advocate these policies but to describe them. In a separate essay written with Rachel Kleinfeld and Phillip C. Bleek for the Sloan Foundation, I propose more extensive steps for increasing citizen preparation.[101] The discussion here hopefully has at least shown that the risks of comprehensive catastrophe and reload demand this preparation.

---

[97] P.T. Bartone and K.M. Wright, "Grief and Group Recovery Following a Military Air Disaster," *Journal of Traumatic Distress* 3, no. 4 (October 1990).

[98] "When business communicated about the health aspects of a crisis to its employees, partners, customers, or the public it improved credibility for business messages to "echo" rapidly the latest public health messaging of the government health officials." Gene Mathews, The Public/Private Response to Sudden Disease Outbreak (Atlanta: The CDC Foundation, 2005), 7, available at <http://www.cdcfoundation.org/sitefiles/TorontoReport.pdf>.

[99] Ibid., 9.

[100] HR 3565 (2005), introduced by Congressman Patrick Kennedy.

[101] Danzig, Kleinfeld, and Bleek, *After an Attack*.

CHAPTER SIX

Surprise, Intelligence, and Vaccines

Surprise

An effect commonly sought by terrorists—and dramatically achieved in the 9/11 attacks—is surprise. Al-Qaeda prides itself on the innovative character of its operations; new tactics are rarely anticipated by police and intelligence authorities.[102]

Proliferating Technology

Bioterrorism is even less predictable than other instruments of terror. Our track record is recurringly poor. No one anticipated mass terrorism by Aum Shinrikyo: both Western and Japanese experts overlooked Aum's experimentation with anthrax.[103] Similarly, when a Rajneeshee cult contaminated salad bars in Oregon, its actions were so unexpected that, though effective, they were not identified as attacks until a year later, and then only after a defector reported them.[104] Our vast and intensely committed Cold War intelligence establishment overlooked a Soviet bio-warfare program that employed 50,000 people over two decades.[105] Our errors of both underestimation (in the 1980s and 1990s) and overestimation (in this decade) in our surveillance of Iraq are now obvious. Reviewing the record, the recent report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction judged our intelligence establishment to be quite deficient in its assess-

[102] Identifying five particularly "worrisome traits" about Al-Qaeda, the "House-Senate Joint Inquiry Report on 9/11" first listed its "long-ranging planning … simultaneous operations … operational security … [and] flexible command structure;" the fifth and last characteristic was "imagination," ed. Steven Strasser, 429–30.

[103] Masaaki Sugishima, "Biocrimes in Japan" in ed. Masaaki Sugishima, *A Comprehensive Study on Bioterrorism* (English Part–Legal Research Institute, Asahi University) (2003), 86ff, esp. 96ff; Hiroshi Takashi et al., "*Bacillus anthracis* Incident, Kameido, Tokyo, 1993," *Emerging Infectious Diseases* 10, no. 1 (January 2004), 117–120; Paul Keim et al., "Molecular Investigation of the Aum Shinrikyo Anthrax Release in Kameido, Japan, *Journal of Clinical Microbiology* 39, no. 13 (December 2001), 4566–4567.

[104] Miller, Engelberg, and Broad, *Germs*, 23. Arguably, the Rajneeshee attacks were not terrorism because the perpetrators hoped to keep them secret.

[105] Scattered intelligence indicators prompted suspicions, but, as with the Rajneeshi, only when a defector (Victor Pasechnik in 1989) became available did higher-level officials grasp the extent and character of the program. Miller, Engelberg, and Broad, *Germs*, 94–7.

ment of Al-Qaeda's pursuit of biological weapons.[106] It went on to approvingly quote "a senior official in the CIA's Counter-Proliferation Division," who said: "We don't know more about the biological weapons threat than we did five years ago, and five years from now we will know even less."[107]

The problem is attributable in part to the generally low visibility of terrorist operations, but in the main it inheres in the instrument of bioterrorism. Pathogens and means of delivering them are very diverse. With the lone notable exception of *b. anthracis* (the pathogen causing anthrax) and the potential crippling catastrophic consequences of using it as an aerosol, no single microbe or mode of attack can confidently be described as much more probable than others. Further complicating prediction, biology and its technologies are changing radically, and this change is accelerating. With each passing year, the possibilities are less predictable.[108] Small laboratories can produce weapons with catastrophic consequences. For each of these reasons individually, and especially because of the combination of all collectively, *we must plan for surprise*.[109]

Planning for surprise is particularly essential to a long-term strategy. The longer the time horizon over which we are attempting to counter bioterrorism, the greater the uncertainty. If the permutations of biological risk at present outstrip our predictive capability, it should be evident that we cannot plan for the future by investing according to particular predictions.

Limits of Prediction

We resist this conclusion, instead talking, planning, and acting as though the world were susceptible to precise description, accurate prediction, and effective control. This tendency is buttressed by our deep embrace of rational thought generally and science in particular.[110] Science, when it is sound, has consistent descriptive, predictive, and interventionist power. We presume that a perceptive understanding of terrorist threats should have the same benefit.

---

[106] "In fact, al Qa'ida's biological program was further along, particularly with regard to Agent X, than pre-war intelligence indicated. The program was extensive, well-organized, and operated for two years before 9/11, but intelligence insights into the program were limited." *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Report to the President* (Washington, DC: Government Printing Office, 2005), 269, available at <www.wmd.gov/report/>. See also: "Indeed, as one Counterterrorist Center official told us, the Intelligence Community 'entirely missed' assessing the size and scope of al-Qa'ida's Agent X program: 'If it hadn't been for finding a couple [of] key pieces of paper [in Afghanistan]… we still might not have an appreciation for it. We just missed it because we did not have the data.'… Despite diligent collection efforts after 1998, it was "remarkable how much [the Community} had not identified [in Afghanistan]," 274. Portions of some of the "pieces of paper" apparently referred to later became public as a result of a Freedom of Information Act Request. See Eric Lipton, "Qaeda Letters Are Said to Show Pre-9/11 Anthrax Plans" *New York Times*, May 21, 2005.

[107] Ibid., 506.

[108] The public summary of a National Academy of Sciences panel convened for the CIA on this subject reported: "The panel noted … the genomic revolution is pushing biotechnology into an enormous growth phase. Panelists asserted that the resulting wave front of knowledge will evolve rapidly and be so broad, complex and widely available to the public that traditional intelligence means for monitoring WMD development could prove inadequate to deal with the threat from these advanced biological weapons." The panel concluded that biotechnology is "likely to advance very rapidly, causing a diverse and elusive threat spectrum. The resulting diversity of new BW agents could enable such a broad range of attack scenarios that it would be virtually impossible to defend against…" Central Intelligence Agency, Directorate of Intelligence, "The Darker Bioweapons Future" (November, 2003), available at <http://www.fas.org/irp/cia/product/bw1103.pdf>.

[109] This is not to say that surprise is inevitable or occurs in all respects. The intelligence community recognized, for example, that anthrax was likely to be a weapon of choice before it became a mainstay of the Soviet program, was tested by Aum, used in the fall 2001 mailings, and pursued by Al-Qaeda. But surprise is such a distinct possibility, even probability, in bioterror attacks that our long-term strategic plans must account for this factor.

[110] The commitment to science is part of the foundation of contemporary Western civilization. The strengths and weaknesses of this commitment are subjects of hot discussion among contemporary philosophers. See generally, for example, Robert Brandom, *Rorty and His Critics* (Malden, MA: Blackwell Publishing, 2000).

But we are pursuing an illusion. At its best, science operates with the benefit of mathematically or empirically demonstrated rules, controlled and replicable experiments, and prolonged and open debate. Even then, error is abundant. Assessing studies that recently appeared in first-rank science journals and were cited more than one thousand times (citation frequency was taken as a surrogate for importance), a researcher reported that significant error was later shown in almost a quarter of well-controlled studies. And when controlled experiments were not the basis of the eminent article, error was the norm; of six such studies in the sample, five were either wrong or significantly overstated.[111] Commenting on these results journal editors observed that scientific debate must:

> … separate data ("in this study, 5% of people examined who lived in San Francisco from 1965–1970 developed lung cancer compared with 20% of people studied who lived in Anchorage") from conclusions ("lung cancer rates are higher in Anchorage than San Francisco") and hypotheses ("cold weather exacerbates the consequences of smoking").[112]

Intelligence

Intelligence analysis is much more prone to error than scientific studies. The "laws of human behavior" are much less predictive than the "laws of science." In any case, no set of laws can ensure valid conclusions, if the data to which the laws are applied are incomplete or inaccurate. Intelligence data are almost invariably fragmentary; data sometimes permit a measure of validation from collateral sources, but they are rarely replicable (and even more rarely replicated) in controlled experiments;[113] intelligence data are subject to strong biases of the collector and the provider—and these problems are then compounded by frequent strong biases of analysts and policymakers; the objects of our intelligence prize secrets and traffic in disinformation (by contrast, nature, the subject of science, at least does not intend to be deceitful); and hypotheses drawn from this data rarely benefit from prolonged, open, and well-informed debate.

In this light, it can hardly be expected that our intelligence-derived hypotheses—so often treated in policymaker and public discussions as though they were conclusions—will routinely be correct. Moreover, even when correct, it will be difficult for them to enlist consensus support and provide a catalyst for action.

---

[111] One researcher studied 45 articles that purported to show efficacy and had received more than one thousand citations. "Five of 6 highly cited nonrandomized studies had been contradicted or had initially stronger effects while this was seen in only 9 of 39 highly cited randomized trials (P=.008)." John P.A. Ioannidis, "Contradicted and Initially Stronger Effects in Highly Cited Clinical Research," *Journal of the American Medical Association* 294, no. 2, (July 13, 2005), 220.

[112] Commenting on Ionannidis' work, the editors of PLoS Med (Public Library of Science Medicine) conclude: "most studies should be viewed as hypothesis generating rather than conclusive." "Minimizing Mistakes and Embracing Uncertainty," PLoS Medicine Editors, e272, (August 30, 2005), 2, available at <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1196486>. Our better intelligence products go some way toward these distinctions by distinguishing "facts" and "judgments."

[113] An instructive case study by Michael Barletta analyzes the evidence that led the Clinton Administration to conclude—almost certainly mistakenly—that the al-Shifa pharmaceutical plant in the Sudan was producing chemical weapons. Among other things, Barletta, drawing on observations from his Monterey Institute of International Studies colleague, Jonathan Tucker, notes that the critical piece of evidence—a soil sample alleged to be from al-Shifa and contaminated with a VX precursor—was not subject to control. Comparison with other samples from the area (but outside the plant) might have shown that the chemical was endemic, for example, from a pesticide. Michael Barletta, "Chemical Weapons in the Sudan: Allegations and Evidence," *The Non-Proliferation Review* 6, no. 1 (Fall, 1998), 115, 124.

These observations apply broadly to strategic intelligence,[114] especially to intelligence about terrorists, and most especially to intelligence about bioterrorism. To enhance our perspective about the power of intelligence with regard to bioterrorism, I suggest the following five thought experiments. In each case, I ask the reader to assume the facts stated in the first sentence and then to address the question posed in the second sentence.

1. A known, intensely analyzed, foreign-based, terrorist group (for example, Al-Qaeda) is pursuing an aerosol anthrax weapon for use in the United States. How would we describe our present confidence (or our confidence after a proposed intelligence system reform) that we would detect this effort, locate it, and intervene to significantly reduce that group's chances of success?

2. A small foreign group (less than a dozen members) that is known but not substantially studied is pursuing an aerosol anthrax weapon for use in the United States. How would we describe our present confidence (or our confidence after a proposed intelligence system reform) that we would detect this effort, locate it, and intervene to significantly reduce that group's chances of success?

3. A small foreign group (less than a dozen members) that is known but not substantially studied seeks to harvest a pathogen from nature (e.g., foot and mouth disease) and disseminate it by simple methods (e.g., exposing cattle by contact with an infected cloth) in the United States. How would we describe our present confidence (or our confidence after a proposed intelligence system reform) that we would detect this effort, locate it, and intervene to significantly reduce that group's chances of success? (Additionally, if a disease were to become evident without prior intelligence indicators, how would we describe our present confidence that we would be able to determine whether the epidemic was intentional or accidental?)

4. An individual scientist (on the model of the Unabomber) inside the United States is trying to establish a "signature weapon" by modifying an existing pathogen to be released in aerosol form and used to further his social agenda. How would we describe our present confidence (or our confidence after a proposed intelligence system reform) that we would detect this effort, locate him, and intervene to significantly reduce his chances of success?

To these I will add a fifth thought experiment that I will put aside for the present but return to in the vaccine section of this paper:

5. Senior American policymakers ask whether we face so substantial a danger from pathogen X as to warrant vaccinating American civilians (recognizing that vaccination, as with smallpox, carries its own costs and risks). What is the likelihood that we will be able to provide an assessment with sufficient confidence and power to convince decisionmakers to undertake this program?

Of course, we rebel against these questions and are inclined to say that they cannot be answered without more context and detail. But it is only by considering how intelligence might be used that we can aptly determine its likely utility. I would suggest that the probability of our success ranges from highest in the first case to the lowest in the fourth and that, over the long term (for example, over the next decade), we are likely to fail in all cases.

What is most interesting about these tests, however, is not the probability of success associated with each, but rather that they may give us some perspective about the extent to which proposed invest-

[114] See generally Richard K. Betts, "Fixing Intelligence," *Foreign Affairs* 81, no. 1 (January/February 2002). We are much better at tactical intelligence, for example, the observation of troop deployments on a front.

ments, reorganizations, and strategies are likely to produce improved outcomes. For example, acknowledging that national biological warfare programs are very hard to discover, and that terrorist programs will be even more difficult to detect, our intelligence community has invested in recruiting and training analysts skilled in microbiology; it has given greater priority to gathering operational intelligence, particularly through surveillance of significant facilities; and it has focused, quite appropriately, on efforts by Al-Qaeda and potentially hostile states to build bioterrorism and biowarfare capability. I think these efforts are commendable because even small gains in our intelligence capabilities will be worth these costs. I believe that they are unlikely, however, to substantially change our performance on the tests that I have mentioned. We should resist the temptation to imply that they will.

To improve our long-term prospects, I would supplement these efforts with changes in the kind (not just in the quantity) of our collection and analysis efforts.

Collection

It has been observed that critiques of intelligence failure commonly emphasize failures in analysis, pointing to clues that lay unnoticed in files.[115] Reorganizations, reassignments of personnel, and increases in the numbers of analysts have accordingly been recommended and, by and large, been embraced. But improvements in our performance against the test cases I have proposed are more likely to depend on improvements in collection than on improvements in analysis.[116]

These improvements must be predominantly in human intelligence (HUMINT). During the Cold War, it was immensely helpful to collection that nuclear and missile facilities and test ranges, large-platform weapons (like ships), and mass troop movements were all subject to aerial and other surveillance. Over the decades our intelligence efforts adapted to this opportunity-rich environment.[117] However, biological facilities and tests are so small and so like innumerable commercial activities that they are not generally subject to detection by comparable technical means.[118] Consequently, there is wide acceptance that human intelligence sources are more likely than technical sources to be successful in tracking biological activity.

---

[115] "When surprise attacks occur, it is rarely claimed that the weak link was the collection link. On the contrary, much of the academic thought on the subject centers on the counter-intuitive thesis, according to which surprise attacks have occurred even in situations where … early-warning information was seemingly abundant. That, for example, is what Roberta Wohlstetter argued in her pioneering work on Pearl Harbor, as did subsequent studies pointing to alleged successful collection in the Yom Kippur War and other familiar examples." Uzi Arad, "Intelligence Management as Risk Management: The Case of Surprise Attack" in Paul Bracken, Ian Bremmer, and David Gordon, *Managing Strategic Surprise: Lessons from Risk Management and Risk Assessment* (New York: Eurasia Group, 2005), 46.

[116] Uzi Arad, a former director of the intelligence division of Mossad and former national security advisor to the Prime Minister of Israel, makes this point about the importance of collection in general: "The investigative reports on 9/11 events and the report of the Senate Committee that dealt with intelligence on Iraq state explicitly that the source of failure was intelligence collection…. [T]he glaring lacunae were at the level of information—its quality, its definiteness, its cleanness and its quantity." Ibid., 48.

[117] The history is well told in Philip Taubman, *Secret Empire: Eisenhower, The CIA, and the Hidden Story of America's Space Espionage* (New York: Simon & Schuster, 2003). See also William Burrows, *Deep Black: Space Espionage and National Security* (New York: Random House, 1987).

[118] Some, but only very modest, gains may be had by tracking equipment and pathogens. Professor George Church has proposed that "All use of reagents and oligos [oligo synthesis machines and supplies] would be automatically tracked and accountable (as is done for nuclear regulations)." George Church, "A Synthetic Biohazard Non-Proliferation Proposal," available in MS Word at <http://arep.med.harvard.edu/SBP/Church_Biohazard04c.htm>. Others have suggested that synthesizers be monitored. However, informal estimates suggest that these number in the tens of thousands. According to a report of the National Intelligence Council, "BW/CW programs will be less reliant on foreign suppliers." *Mapping the Global Future: Report of the National Intelligence Council's 2020 Project* (Washington, DC: Government Printing Office, December 2004), 100, available at <http://www.dni.gov/nic/NIC_2020_project.html>.

But our collection programs cannot be made substantially more successful predominantly by expanding our agencies, our targets, and the desired specialties of our spies. The paradigm underlying our human intelligence system also has to change. In our confrontation with the Soviet Union, by and large, we knew who the generals, scientists, and foot soldiers of the enemy were and where they were. Indeed, some of our strongest warning indicators were variations from previously observed routines (for example, failures to disperse after training exercises, or sending submarines from bases at unusual times or in unusual numbers).[119] The challenge was not so often to identify or even to locate the enemy as it was to determine what they were trying to do and how they were doing it. To meet this challenge we designed our HUMINT systems, no less than our technical systems, to cope with targets of concern that were largely inaccessible. Skilled and courageous intelligence officers represented our best, and often our only, route to personal contacts with potential sources. Frequently these were clandestine contacts.

Over the next decade the conditions for the collection of HUMINT against bioterrorists will sometimes be like those that characterized Cold War targets. To the extent that terrorists can be identified and induced to become informants, or that other informants can help us, contacts made by our agents will yield invaluable information.[120] But usually the situation will be different. We will generally have a pretty good idea of what terrorists are trying to do, and in some cases we will be able to identify them, but in many cases will not know whom we should focus on or be able to locate them. Jeffrey Cooper put the point this way:

> we need to fundamentally rethink our paradigm for warning from primarily a monitoring process built on established patterns and narrowly focused on few targets of interest to a discovery process of wide-ranging scanning, including recognizing anomalies against less familiar backgrounds.[121]

Cooper offers a helpful analogy when he suggests that the transition that is required is like that of moving from focused vision (our method of Cold War intelligence) to peripheral vision.

> Peripheral vision covers a very wide field of view, it is particularly sensitive to motion and certain other cues at the very edges of the vision field, and, as an autonomic function, scans the surrounding environment involuntarily; on the other hand, it is monochromatic and lacks the ability to discern fine detail.[122]

In seeking the sources of bioterrorism, this "wide-ranging scanning" or "peripheral vision system" will try to discover scientists and technicians who operate laboratories or undertake tests without evident sources of support, pursue research without publications or presentations, seek pathogens or

---

[119] See generally Cynthia Grabo, *Anticipating Surprise: Analysis for Strategic Early Warning* (Lanham, MD: University Press of America, 2004).

[120] The Madrid bombing ring was, for example, monitored by a police informant because of the close connection some of its members had with drug trafficking. Unfortunately, relocation of the informant and failures in follow-up left the plotters free to proceed. Even then, detection after the bombings was significantly aided by informant information.

[121] Jeffrey R. Cooper, "Towards More Effective Warning through Peripheral Vision: Effective Anomaly Detection and Resolution" (SAIC, unpublished manuscript, 2005), 4. See also, Jeffrey R. Cooper, "Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis"(2005), 19, available at <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/curing-analytic-pathologies-pathways-to-improved-intelligence-analysis-1/index.html>.

[122] Ibid., 5.

protective gear not relevant to their regular duties or evident commercial purposes, consort with questionable actors, etc.[123]

This calls for a different approach, one that complements our traditional emphasis on targeting and monitoring by using a broader net that encompasses more possibilities. The predominant components of that net will not be CIA case workers operating clandestinely; rather, they will be civilians making open commercial and academic contacts in professions relevant to bioterrorism. To be effective in the context of such broad uncertainty, our analysts need to engage in what Peter Schwartz calls "strategic conversations"[124] with experts outside our intelligence establishment. If intelligence agency and civilian assets can be brought into better coordination with one another, our collection will substantially improve.

The argument for this coordination begins with the simple fact that case officers will never be numerous enough to track the universe of those knowledgeable enough to have a reasonable prospect of making biological weapons if they are committed to that task. I have estimated that the latter population is likely to number in the millions.[125] By contrast, the CIA's Deputy Director for Operations has testified that "we cover a terrorist target around this globe using a cadre of case officers that is smaller than the number of FBI officers who work in New York alone."[126] This and other comments suggest that we have fewer than 1,000 case officers abroad and focused on terrorism at any given time.[127] Without a strong ability to identify the source of a threat, the haystack of biological work is simply too large, and the needles of terrorist work too small, to ever offer a substantial likelihood of success.[128]

The key to improving our performance lies in harnessing the army of Americans knowledgeable about biological activities employed in our universities, pharmaceutical, biotechnology, and agricultural companies, hospitals, veterinary centers, domestic and international public health organizations, and their foreign counterparts.[129] Using contemporary models of distributed teams, our aim should be to harness the power of numbers, linking elements of the broader population in a network

---

[123] While nation-states have been able to keep biowarfare programs secret by employing weaponeers behind a façade of self-contained biodefense and other national activities, terrorist groups will not have analogous capabilities. It would be a significant additional burden for them to build a completely separate structure as, for example, the Soviet Union did. Instead, terrorists are likely either to physically hide people engaged in developing biological weapons or to veil their activities in contexts where they are likely to have law-abiding colleagues, suppliers, and often even supervisors.

[124] Peter Schwartz, *Inevitable Surprises: Thinking Ahead in a Time of Turbulence* (New York: Gotham Books, 2003), 229.

[125] For my more detailed estimates of the relevant populations of "weaponeers" and "broadly skilled" personnel capable of making biological weapons over the course of 1–2 years, see Richard Danzig, *Proliferation of Biological Weapons Into Terrorist Hands*, paper prepared for the Aspen Strategy Group (2004), 16–17.

[126] James L. Pavitt (Deputy Director for Operations of the CIA), "Written Statement for the Record on Weapons of Mass Destruction (WMD) Programs," before the National Commission on Terrorist Attacks Upon the United States (April 14, 2004), 2–3.

[127] In 2003, Senator Charles Schumer's office reported that there were 1,074 FBI agents in New York City. <http://schumer.senate.gov/SchumerWebsite/pressroom/press_releases/PR01664.html>. A 2005 newspaper article offered a higher (though less authoritative) estimate that there were 5,000 CIA case officers, of whom between a third and a half were abroad at any one time. Walter Pincus, "Goss Plan to Strengthen CIA is Ready," *The Washington Post*, February 16, 2005, A2, available at <www.washingtonpost.com/wp-dyn/articles/A27348-2005Feb15.html>. The two reports may be compatible if we assume that the *Washington Post* estimate is for all case officers and approximately half of those are focused on terrorist activity.

[128] It is also unlikely that government employees would have the time, taste, and talent to remain abreast of cutting-edge developments that might be misapplied to generate unprecedented threats.

[129] See also, Amy Sands, "Integrating Open Sources into Transnational Threat Assessments," in *Transforming U.S. Intelligence*, ed. Jennifer Sims and Burton Gerber (Washington, DC: Georgetown University Press, 2005), 63 ff: "The intelligence community has had a hard time recognizing the value of open sources and then using them." See also, in the same volume, Henry A. Crumpton, "Intelligence and Homeland Defense," 198 ff, urging that the intelligence agencies achieve a "Partnership with America," 213.

so that people at the edge of the net educate those at the center without being directed by them.[130] These non-intelligence professionals, now only serendipitously connected to our intelligence establishment, can systematically provide insights into people, equipment, technology evolution, and natural conditions that may be linked to bioterrorism.

In many contexts, our private citizens will be a more likely source of insight than our intelligence employees. Traditions, pressures for efficiency, and strong pressures to minimize risk are likely to dispose agency operatives against general surveillance of probably benign individuals and institutions, even if it is accepted that some of these may be sources of surprise. Case officers are rewarded for developing fruitful sources and insights. Years spent looking for individuals or small groups pursuing biological weapons at a targeted Middle Eastern or South Asian university are likely to be both unrewarding and unrewarded. Agencies are unlikely to attract and retain quality personnel to sustain these efforts.

Moreover, personal relationships are central to detecting aberrational behavior. If someone who is not malevolent suspects that the behavior of an acquaintance or colleague is aberrational, it is not likely that he or she will report the matter directly to an intelligence agency. A Russian scientist, for example, who is concerned that an underpaid colleague may be helping terrorists cannot be expected to pick up a phone or send an email to a state intelligence agency, much less the CIA. But a scientist may mention his suspicions to a sympathetic colleague, and if the profession is profusely populated with individuals who are concerned about bioterrorism and have relationships with the relevant agencies—or with others who have these relationships—word may well filter back to the right quarters.[131] The critical variable will be how richly the relevant professions are populated with these individuals.

---

[130] See generally von Hippel, *Democratizing Innovation*. Linux and Apache Web (which now runs some 70 percent of internet domains) are examples of the software applications of this principle.

There are examples of the application of this model in government and private efforts to detect terrorists. FedEx is "encouraging its 250,000 employees to be spotters of would-be terrorists. It is setting up a system designed to send reports of suspicious activities directly to the Department of Homeland Security via a special computer link…. Federal agents privately praise Western Union for sharing information with Treasury and Homeland Security investigators about overseas money transfers." Robert Block, "Private Eyes: In Terrorism Fight, Government Finds a Surprising Ally: FedEx; Since 9/11, Firms Cooperate More Often With Officials; Implications for Privacy; UPS and the Post Office Balk**,"** *The Wall Street Journal,* May 26, 2005.

[131] Prof. Dean Wilkening of Stanford University makes a similar point. "The Soviet biological weapons program would have been more difficult to conceal had there been international collaboration with Soviet biologists, medical and public health practitioners during the Cold War." *Encyclopedia of Violence, Peace, and Conflict* (Amsterdam: Academic Press, 2008).

It must be noted, however, that reliance on relationships is, like other mechanisms, an imperfect strategy. In an informative account by the head of Iraq's clandestine nuclear program, Dr. Mahdi Obeidi relates his strong sentimental ties to his alma mater, the Colorado School of Mines, and to his American "college sweetheart" there. He describes a nostalgic visit to the campus and dinner with this woman, who, with her mother, was "like a second family to me." The author recounts his "melancholy" at hiding the realities of his work from these friends, but "the need for deception" dominated his conduct. Mahdi Obeidi and Kurt Pitzer *The Bomb in My Garden: The Secrets of Saddam's Nuclear Mastermind* (Hoboken, NJ: John Wiley & Sons, 2004), 82–84.

Another instance involving nuclear proliferation illuminates additional difficulties: Dr. Abdul Quadeer Khan initiated his nuclear bomb development activities on behalf of Pakistan by stealing classified information from URENCO, an international consortium that built centrifuges in, among other places, the Netherlands. A close Dutch friend, Frits Veerman, was apparently aware of many of Dr. Khan's irregular practices but took a long time to realize what was happening. William Langewiesche, "The Wrath of Khan: How A.Q. Khan made Pakistan a Nuclear Power—and showed that the spread of atomic weapons can't be stopped" *The Atlantic Monthly* (November 2005), 62 ff. Langewieswche reports Veerman as saying that, "everything seemed so aboveboard—so normal and brightly lit —that Veerman was mostly just glad to have this friend," 71. Moreover, when Veerman eventually developed suspicions and reported them to a superior "[t]he manager was visibly skeptical. He later got back to Veerman, scolding him that such allegations were too serious to be made without proof, and advising him not to stir up trouble at the lab. [The organization] was overcome by institutional inertia," 72.

In some contexts, we have cultivated these sensitivities and the relationships that are likely to lead to reporting. Notably, for example, the Nunn-Lugar legislation and related State Department initiatives have funded well-designed programs that support commercial efforts by Russian and Former Soviet Union nationals who previously worked in bio-weapons facilities.[132] Where these efforts lead simply to a transfer of funds, there is no reason to believe that they will buy loyalty. Where, however, they lead to personal relationships,[133] experience and more formal assessments suggest that the relationships will encourage greater adherence to international norms and transmission of information.[134]

Unfortunately, other arenas of potential relationship are being ignored or, worse, stifled. The pharmaceutical industry, for example, is dominated by western companies with widespread sales networks, but salespeople are not systematically sensitized to indicators of concern or encouraged to work in contexts that may lead to insight abroad and to debriefing at home. The biotech industry is predominantly American,[135] but its executives are largely out of touch with our national security establishment. Our universities are centers of training. The closest international relationships are frequently those between professors and their former students. But our post-9/11 visa and funding policies discourage bringing foreign students and scientists to America for training in biology.[136] A wiser, long-term strategy would recognize the globalization of science; it would build, rather than discourage, relationships between Americans and foreigners, it would systematically establish relationships with those who have these contacts, and it would provide our agencies with the benefit of this information.

---

[132] See generally Kenneth Luongo and William Hoehn III, "Reform and Expansion of Cooperative Threat Reduction," *Arms Control Today* 33, no. 5 (June 2003).

[133] A reader of this paper commented that Russian scientists he worked with "learn to trust us over years. Now 5 years into the engagement, we fly them to [the U.S.] for life-saving cancer therapy, they share thanksgiving holiday at our house, meet our wife, pet our dog, and we take care of their college-aged sons and daughters who are training in our universities. This evokes a level of disclosure about weapons related topics that is difficult to replicate."

[134] I advanced this conclusion in *Proliferation of Biological Weapons Into Terrorist Hands*. There I noted that: "I derive this judgment from conversations with those centrally involved in the effort and from one commendably precise, though limited, analysis. At the end of 2003, Deborah Yarsike Ball and Theodore P. Gerber employed a Russian survey firm to query 603 Russian physicists, chemists, and biologists about their willingness to entertain job offers from a number of countries, including North Korea, Syria, Iran and Iraq. "Will Russian WMD Scientists Go Rogue? Measuring Russian Scientists' Willingness to Work in High-Threat Countries and the Impact of ISTC" (Unpublished Lawrence Livermore National Laboratory study for the State Department Science Centers Program, January 2004). They found that "*20% of our sample would consider taking a job in at least one high-threat country,*" 5. (Italics in the original.) They recorded substantial differences between the general sample and those who were "principal investigators" on Nunn-Lugar grants—only seven percent of those investigators described themselves as open to employment elsewhere. (These results remained significant when variables of age, income, and status were controlled for.) On the other hand, they observed no significant differences between those who participated at a lesser level in grant programs and those who did not participate at all: "ISTC participants who are not project managers are only slightly less likely than those who never applied at all to ISTC (19 percent versus 23 percent) to demur from the chance to work in a high-threat country," 6.

[135] Ernst and Young reports that the geographical distribution of the industry was essentially stable in 2004 as in 2003. "The United States still dominated the field, accounting for 78% of global public company revenues…," 11. While private foreign companies outnumbered their U.S. equivalents by 3 to 1, 137,000 of the 184,000 biotech employees worldwide worked for U.S. companies. Ernst and Young, *Beyond Borders: Global Biotechnology Report 2005*, available at <www.ey.com/global/content.nsf/international>.

[136] For data and recommendations offered from the standpoint of trying to enhance U.S. economic competitiveness, see National Academy of Sciences, *Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Future* (Washington, DC: National Academies Press, 2006), Appendix IS, "International Students and Researchers in the United States."

Assessment

At a higher level, because of their range of interests, travels, and contacts, leaders of "big pharma," biotech, biology-oriented venture capital firms, the international public health community, and academia are our best advisors about the possibilities of pathogenic surprise, whether from natural or malevolent causes.[137] As a general rule, they have very close relationships with one another but minimal relations with our national security agencies. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction reported that "CIA analysts observe that their agency in particular does a poor job of interacting with outside experts."[138] Interactions between our security experts and those active in biology are particularly poor.

Alan Beyerchen, a historian at Ohio State University, has suggested that World War I brought the chemists into government; World War II did this for physicists; the Cold War did the same for computer and telecommunications experts; but this transition has not occurred for biologists.[139] Physics, chemistry, computer sciences, and telecommunications are now all perceived as central to national security and have accordingly been substantially funded by the Department of Defense, the Department of Energy, and the intelligence agencies. Physicists, chemists, computer, and telecommunications experts routinely serve in high and middle positions across government. No such relationships exist for biologists.[140]

There are more than a score of relevant, government-established advisory boards that attract biologists,[141] but these boards typically meet rarely or for a limited term with a limited focus (they do not engage in Schwartz's "strategic conversation"); they do not draw from a wide spectrum of experience and expertise (participation rarely involves the pharmaceutical industry and those younger than 50); members have low-level, or frequently no, security clearances; they are unpaid, untrained, and only minimally supported by staff; their board activities are added to their "day jobs," usually not valued by their home institutions, and not productive for their careers; preparation for meetings is minimal; discussions are either very narrowly focused or so general as to produce only occasional insight. There has been no group of academic and industry based biologists that is cleared for compartmented information, supported by paid staff, regularly informed of intelligence developments, regularly consulted about scientific developments, and invested in independent thinking before meetings and collaborative thinking during them.

---

[137] As a valuable rare example of the rewards of collaboration, see James B. Petro and David Relman, "Public Health: Understanding Threats to Public Openness" *Science*, 302 (December 12, 2003), 1898. The collaboration between Petro (a Defense Intelligence Agency microbiologist) and Relman (a Stanford Medical School Professor) better focused attention on the Al-Qaeda investments in bioterrorism that were generally overlooked, as noted in footnote 62.

[138] *Commission on the Intelligence Capabilities of the United States*, 509.

[139] The Beyerchen statement and a discussion of it are available at <http://www.chetrichards.com/modern_business_strategy/moore/mie_31.htm>

[140] Another manifestation of this perspective is that while physics and chemistry are central to the curricula at military service academies, biology is not available as a course offering for any but pre-med students at West Point.

[141] There is no lack of entities, all essentially uncoordinated. I note, for instance, the Central Intelligence Agency's Intelligence Science Board, the Defense Science Board, the Defense Intelligence Agency's 2020 Panel, the Science Panel for SOCOM, the FBI Science Board, National Biodefense Analysis and Countermeasures Center (NBACC) science advisory groups, the State Department Advisory Committee on Counter-Proliferation, the recently formed National Science Advisory Board for Biosecurity, and a number of National Academy of Sciences government-sponsored committees, panels, and forums (including its Committee on International Security and Arms Control, its Panel on Biological Threats, its Forum for Microbial Threats, and several panels for biology related country "dialogs" [U.S.-Russia, U.S.-China, etc.]). The Jasons, a longstanding body, predominantly of physicists, have, by request, conducted occasional studies of biology topics.

After hearing statements to this effect from a number of observers, the Commission Regarding Weapons of Mass Destruction concluded that "the culture gap between the biological science and defense communities is so large that housing them together is essential to fostering a common strategy."[142] The Commission recommended creating:

> [an] elite Biological Sciences Advisory Group, administered by the DNI's Director of Science and Technology, which would be composed of the nation's leading life science experts. The group would be compensated for their work and asked to examine and advise the DNI on biological threats;[143]

This advisory group, very much of a piece with my own urging of a "Case X Committee" two years ago,[144] should convene regularly to discuss developments in intelligence, scientific technology,[145] and the natural environment that may presage catastrophic bioterrorism or a natural pandemic.

Since these recommendations, the Director of National Intelligence has taken steps to create just such a national advisory group, calling it a Biological Security Experts Group (BSEG). This valuable initiative should bring us some of the advantages of a "Case X Committee," especially because its members are being given clearances and will meet regularly. However, because members are only minimally compensated, staff support is limited, and meetings are as frequent as two days per month, this effort is likely to substantially engage only those who are already committed to work on bioterrorism. To be fully beneficial the BSEG will need to engage broader representation from the pharmaceutical, biotech, academic, and public health communities, be paid, and be supported by more than a single staff person (as at present). Most significantly, this body should not simply evaluate intelligence. In addition to its functions in diminishing surprise, it should channel talent to subsidiary sciences advisory boards and be represented on the biology council described below.

Far from being radical, a body that actively connected industry and government would merely be a step toward restoring some of the close biology-government relationships that existed during World War II.[146] At that time a reserve unit was manned by scientists from Merck and other pharmaceutical companies. George Merck took a leave from the presidency of his company to direct the innocuously named War Research Service responsible for America's biowarfare research.[147] The World War II relationships with biologists, however, were transitory.

---

[142] *Commission on the Intelligence Capabilities of the United States,* 509.

[143] Ibid., 511.

[144] "Recommendation 3: Establish a 'Case 5 Committee' [later renamed Case X by the Department of Homeland Security] of scientists from government, academia and biotech and pharmaceutical companies, as well as intelligence officers. Direct the committee to review, at least semiannually, the evolution of biology and of terrorist individual, group and state capabilities and activities in this arena. Have the committee identify indicators and warnings of the evolution of new threats, recommend intelligence efforts to document the evolution of those threats, and change the cases as warranted over the years ahead," Danzig, *Catastrophic Bioterrorism: What is To Be Done?*, 6. (The cases referred to are discussed in part III.)

[145] See e.g., Mark Wheelis, "Will the New Biology Lead to New Weapons?," *Arms Control Today* 34, no. 6 (July/August 2004). Dr. Wheelis, a microbiologist, sees such weapons as arising from "new technologies" including "genomics, proteomics, micro-array technology, high-throughput screening techniques, combinatorial methods in chemistry and biology, site-specific mutagenesis, knock-out mice, and many others."

[146] These in turn were a subset of Vannevar Bush's larger commitment to engaging scientific talent in the war effort. Indeed, it could be argued that one of the strengths of the CIA and its predecessor agency, the OSS, during their early years was that they were composed by bringing people from all walks of American life into the intelligence community. We have sacrificed range as we have established lifetime career paths and deepened professionalism within that community.

[147] See generally Kendall Hoyt, "Vaccine Innovation: Lessons from WWII," *Journal of Public Health Policy*, 1, 27 (Spring 2006), 35–57.

> The organization was built on a temporary basis, drawing upon the best available men for relatively short periods of time … Once the pressure of war lifted, the key men upon whom its success depended responded to the more urgent calls of their regular activities and not all the king's horses nor all the king's men could hold the group together.[148]

The challenge now will be greater. It will be to build an organization to buttress a long-term strategy, and to do so *in advance of* any attacks (possibly powered by reload and stimulating risk contagion) that usually are needed to catalyze a sense of urgency.

Recognition of the diversity of possibilities in biological terrorism and, therefore, of the risks of surprise should lead us to use a BSEG or Case X Committee in a manner different from traditional government advisory groups. In those groups, consensus is valued and opinions are typically developed by interactions among the participants, who are first exposed to data and issues in the course of discussion. The BSEG should strive for the opposite: members should be fully informed about an issue and mandated to think about it and evolve their opinions in isolation from one another in advance of meetings. Diverse opinions, separately considered and derived, are one of the best methods of anticipating surprise. Meetings should then be devoted to a comparison of views, with participants from the private and public sectors educating one another about possibilities. Properly run, a group will achieve a balance that no individual expert could.[149] However, in addition to reporting consensus judgments of the committee, meeting reports should display and honor the diversity of views that remain after this discussion.

Creating a distributed intelligence network performing both collection and analysis and a committee that builds deep connections between industry, academic, and government communities will be difficult. Legal, cultural, and practical barriers exist on both sides of the equation. In my judgment, however, the effort is imperative and potentially richly rewarding.

Vaccine Development

Our vaccine system depends on prediction. Historically, vaccines have been designed to cope with diseases that are either present or thought to be imminent. The system is beset by many difficulties—among them, low investment (both by government and the pharmaceutical industry), low profitability, unstable and limited markets and customers, shortages of skilled personnel and facilities, challenges in vaccine discovery, challenges in manufacturing, difficulties in transitioning from discovery to development to production, delays and uncertainties associated with FDA approval, liability risks, and psychological resistance among potential recipient populations. But when the system works, as it does annually in preparing for influenza, it proceeds as follows: a pathogen of concern is identified; investments are made in research for antigens that can stimulate an immune response protective against that pathogen; mechanisms that work *in vitro* are advanced through pre-clinical and clinical tests; one or more vaccines are demonstrated to be safe and effective; these are approved by the FDA; they are then rapidly manufactured in quantity; once produced, they are broadly administered to at-risk populations or stockpiled or both.

---

[148] Irvin Stewart, *Organizing Scientific Research for War: The Administrative History of the Office of Scientific Research and Development* (Boston: Little, Brown, and Company, 1948), 320, quoted in Hoyt, op. cit. And see Jennet Conant, *Tuxedo Park: A Wall Street Tycoon and the Secret Palace of Science that Changed the Course of World War II* (New York: Simon & Schuster, 2002), 285.

[149] See generally Surowiecki, *The Wisdom of Crowds*.

The understandable tendency is to adopt this model to address national security vulnerabilities as well as natural risks. This approach worked well during World War II. As Kendall Hoyt and I have observed:

> Wartime programs contributed to the rapid development of new or significantly improved vaccines for influenza, pneumococcal pneumonia, Japanese encephalitis, plague, tetanus, typhus and yellow fever. A targeted R&D program permitted rapid development of the Japanese encephalitis vaccine in anticipation of a land invasion of Japan[150] and a botulinum toxoid for D-Day in response to OSS reports that the Germans may have loaded V-1 rockets with the toxin.[151]

As the bioterrorism problem loomed large for the military in the late 1990s and for civilians after the 2001 anthrax attacks, DOD resorted to the same strategy. Among others, it targeted development work around priority pathogens and toxins—anthrax, smallpox, tularemia, botulinum, and Ebola.[152] An expert panel established by DOD in 2001 articulated the prevailing wisdom:

> Vaccines, coupled with effective immunization policy for safeguarding the force from biological warfare agents, are the most effective technological method for enabling successful force projection to any global region where vital interests of the United States are contested…. It is a policy imperative that vaccines—regardless of their source or manufacture—that are intended for force health protection are licensed by the Food and Drug Administration (FDA).[153]

This model cannot be sustained, however, as a means of countering bioterrorism if we accept unpredictability and surprise as dominant characteristics of the bioterrorist risk. In a world of surprise, very few vaccines can be justified, because very few threats stand out from the mass of possibilities. Anthrax, to be sure is uniquely threatening. A case could be made for development and stockpiling of an aerosol plague vaccine. Our work on smallpox vaccines has already been so extensive that the relatively small incremental effort associated with developing an improved vaccine can be justified. But beyond that, the evidentiary base for predicting a particular pathogen is so weak that even if we could provide a rationale for vaccine development, it is hard to imagine that we could justify spending hundreds of millions of dollars on stockpiling and then (because of shelf-life expiration) resupply of the vaccine, much less a policy of administering it—even to troops[154]—in advance of an attack.

---

[150] *U.S. Army Activity in the U.S. Biological Warfare Programs*, vol. I (Washington, DC: U.S. Department of the Army, February 24, 1977), reprinted in Biological Testing Involving Human Subjects by the Department of Defense, 1977, Hearings before the Subcommittee on Health and Scientific Research of the Committee on Human Resources, March 8 and May 23, 1977, United States Senate, 95th Congress, First Session.

[151] Richard Danzig and Kendall Hoyt, *Recommendations for a DoD Vaccine Program* (paper prepared for the DARPA Special Projects Office, 2005). Hoyt gave expression to our views in "Bird Flu Won't Wait," *New York Times*, March 3, 2006. A more general indication of the success of the military program is the fact that the military made significant contributions to the development of vaccines for 18 of the 28 diseases for which vaccines were licensed over the course of the twentieth century. See table 4, chapter 1, Kendall Hoyt, *The Role of Military-Industrial Collaboration in the History of Vaccine Innovation*, unpublished thesis, MIT, May 2002.

[152] At the same time, the Department of Health and Human Services gave vaccine development priority in the National Institute for Allergy and Infectious Diseases.

[153] *Report on Biological Warfare Defense Vaccine Research & Development Programs* ("The Top Report") (Washington, DC: Department of Defense, July 2001), 1, available at <www.defenselink.mil/pubs/ReportonBiologicalWarfareDefenseVaccineRDPrgras-July2001.pdf>.

[154] Witness the resistance to anthrax vaccination.

As some experts have urged, a different model is required.[155] Instead of investing in expensive, late-stage development, licensing, and stockpiling of vaccines narrowly targeted against specific pathogens, this approach would invest our scarce resources in buttressing capabilities that will speed our reaction to broad classes of pathogens. We will focus on building a standby rapid response and surge production capability that can be called upon when a particular pathogen is released, otherwise is identified as an imminent threat, or arises naturally.[156]

A program of this kind would have two preparatory priorities: a medical and biological research component and, no less significantly,[157] a bureaucratic and logistical arm. The first aspect of this effort would shift support from specific pathogens to broadly applicable topics that are now only marginally supported: understanding host-pathogen-drug interconnections,[158] rapidly discovering antigens, validating animal models, constructing multi-functional vector platforms, creating an inventory of scaffolds[159] and adjuvants,[160] boosting non-specific, innate immunity,[161] shortening the time required to achieve protective immunity,[162] improving the "take rate" of vaccination, and achieving less intrusive, faster, and more efficient modes of vaccination.[163]

Insofar as this program funded work on specific pathogens, it would be predominantly to focus on them as representatives of the class of cases of concern. For example, the program might target a virus (e.g., Rift Valley Fever), a toxin (e.g., ricin), and a bacterium (e.g., plague). But the aim would

---

[155] The argument that follows was previously advanced in Danzig and Hoyt, *Recommendations for a DoD Vaccine Program*, from which much of the following material is drawn.

[156] We urged this approach in Danzig and Hoyt, *Recommendations for a DoD Vaccine Program*. An expert group assembled by the Chemical and Biological Arms Control Institute argued for a similar approach, though they put the point more weakly and advanced it only among many other more traditional propositions: "Adaptability is required because new diseases such as SARS, Ebola, and West Nile Virus have appeared unexpectedly in recent years. Likewise, because the life sciences continue to advance at an incredible pace, novel and unforeseen biological agents could be created. Therefore a vaccine infrastructure that is adaptable and can be applied to unknown biological risks that may emerge either naturally or deliberately will be essential. This could be a case for emphasizing the development of platform and other enabling technologies." *Meeting the Biodefense Challenge: A Roadmap for a National Vaccine Strategy* (Washington, DC: Chemical and Biological Arms Control Institute, November 2004), 12.

[157] This point bears emphasis, because the tendency within government and academia is to emphasize the exciting, breakthrough potential of basic research in the new biology while slighting more mundane, but potentially highly profitable, investments in the more applied sciences affecting development, testing, manufacturing, and delivery systems.

[158] Including pharmacogenetics (that is, the study of the relationship between the genetic composition of individuals and their varying susceptibilities to disease) and pharmacokinetics (the study of what happens to drugs in the body).

[159] These platforms would address a conserved component in a broad spectrum of pathogens while permitting an additional component to be "swapped" onto the platform to allow for specific activity against a unique pathogen.

[160] Some adjuvant techniques not now used in the United States because they are painful or have collateral effects would be useful in an emergency. A strengthened inventory of these methods (for example, murano dipeptides, now commonly used in WHO vaccines, but thought to be too uncomfortable for the mainstream U.S. market) would be useful.

[161] This has been a focus of Russian research, for example on interferons, for many years. DARPA's Defense Sciences Office and the National Institute for Allergy and Infectious Diseases have initiated some work along these lines. As with any novel line of research, results cannot confidently be predicted. This difficulty is increased in dealing with issues of innate immunity, because animal models are less relevant, since responses are particularly host dependent. Moreover, to the extent efficacious methods for stimulating cytokines or other defenses are developed, they can be expected to raise risks of auto-immune reactions. These efforts, however, more directly than traditional programs address problems of unpredictability and, accordingly, should be given higher priority.

[162] Including shortening the time to achieve protection with a single dose. (The present anthrax vaccine is thought to take 35 days before it is effective and requires multiple subsequent boosters to achieve long-lasting protection.

[163] For example, through nasal sprays and skin patches. See, for example, Richard Kenney et al., "Induction of Protective Immunity Against Lethal Anthrax Challenge with a Patch," *Journal of Infectious Diseases* 190, no. 4 (August 15, 2004), 774–782: "The present study has demonstrated the feasibility of vaccination using a patch to defend against a present bioterrorism threat," 779. See also Laura Bonetta, "Edible Vaccines: Not Quite Ready for Prime Time," *Nature Medicine* 8, no. 2 (February 2002), 94–97.

be, at least minimally, to develop scaffolds for vaccines against multiple strains of different types of pathogens and, more ambitiously, to develop broad-spectrum antivirals[164] or immune boosters of general applicability.[165]

In its second branch—its efforts to improve bureaucratic, manufacturing, and logistical performance—this program would emphasize reducing the cost and time required for vaccine development and manufacturing,[166] principally by pre-positioning design and production resources to build drugs and vaccines on short notice, creating modular, scalable, fast production systems, establishing policy agreements for authorizing drugs with less than usual safety and efficacy data in the event of a certified emergency,[167] and leading our bureaucracies to develop effective processes, plans, and procedures for rapidly delivering vaccines pre-event to high-risk emergency and essential workers, and post-event to those at risk for exposure.

An agile program of this kind would not aim for traditional, large-scale vaccine outputs and therefore would differ from the efforts likely to be initiated under the present system. Such a program would be largely unclassified and equally concerned with and no less relevant to natural than to weaponized pathogens. It would likely be of considerable interest to drug companies, which would be free to use its results in their commercial efforts. A well-run program should be able to manage research and development on the model of the Very High Speed Integrated Circuit (VHSIC) program run by the Department of Defense and the semiconductor industry in the 1980s. With drug industry cooperation, the program could embrace the development of common tools, as Sematech did in the 1990s. It could establish surge production understandings on the model under which the Defense Production Act[168] established analogous capabilities for weapons, munitions, and equipment during the Cold War.[169]

Initial moves in this direction, have occurred.[170] Through its Defense Threat Reduction Agency, the Department of Defense, for example, announced that it aimed to spend $100 million in 2006 on:

---

[164] See, for example, E. De Clercq, "Cidofovir in the treatment of poxvirus infections," *Antiviral Research* 55, no. 1 (2002), 1–13, and N.J. Snell, "Ribavirin–Current Status of a Broad Spectrum Antiviral Agent," *Expert Opinion on Pharmacotherapy* 2, no. 8 (August 1, 2001), 1317–24.

[165] This would require extensive research. Within the acquisition portion of the Office of the Secretary of Defense, the Directorate for Medical Counter-Measures has identified a half-dozen possible drug and vaccine "solutions" as worthy of substantial present effort: "block key receptors, inhibition by small molecules, modulate immunity, change gene expression, block protein actions, modulate physiologic impacts."

[166] For example, we should invest in accelerating and broadening the movement from chicken eggs to tissue culture as a medium for viral growth and in improving the techniques of recombinant fermentation required for vaccines against botulinum and ricin.

[167] As authorized under Bioshield I.

[168] 50 USC App 2061. See also, "The Strategic and Critical Materials Stockpiling Act," 50 USC A98.

[169] Originally passed to meet Korean War requirements, the Defense Production Act elicited surge production plans from over 10,000 producers in an effort to assure that material deficiencies that had recurred in every American war did not afflict us in the future. In this light, our present inability to produce vaccines in advance of need is of a piece with a longstanding American military challenge. See Jacques S. Gansler, *The Defense Industry* (Cambridge, MA: The MIT Press, 1980): "America's planning for industrial mobilization has always been inadequate…. In the early months (or even years) of conflicts, the United States has always been able to mobilize troops far faster and more effectively than it has been able to arm them," 109. And see James A. Huston, *The Sinews of War: Army Logistics 1775–1953* (Washington, DC: Office of the Chief of Military History, 1966): "Following its practice in all wars, the United States on the eve of World War II mobilized troops before weapons and equipment could possibly be available for them," 455.

[170] DARPA's Defense Sciences Office has been a strong proponent of this approach. Klaus Schafer, recently the Deputy Assistant to the Secretary of Defense for Chemical and Biological Defense, also advocated this strategy, among other things securing financial support for the Broad Agency Announcement cited in the next footnote.

> identifying common structural elements of specific agents or classes of agents (preferred), elucidating common virulence mechanisms (such as type III secretory proteins), identifying functional domains in toxins and virulence factors, and using this information to develop rapid and effective medical countermeasures protecting against genetically engineered or emerging BW threats.[171]

The National Institute of Allergy and Infectious Diseases has similarly allocated a small part of its budget to these broad-gauged initiatives. DARPA's Defense Sciences Office has commendably announced and funded a challenge to drug manufacturers to develop and demonstrate a capacity to produce three million doses of vaccines within 12 weeks while meeting good manufacturing practice standards.[172] To be sustained and broadened to a comprehensive program, a strategy of this kind would have to have national visibility, some consensus support in Congress, a clear mandate on the model of our nuclear submarine program or Manhattan project, and an advocate like Admiral Rickover or General Groves.

This alternative model should not be taken as a panacea. This is a program for the long term. Our recent experience shows a "gap of 10 to 30 years between discovery research and pharmaceuticals being prescribed by physicians."[173] Our aim is to move much faster, but even if our speed were tripled, achievement in this arena would take us 3–10 years. Failures will be prevalent. Many diseases have been targeted for many years, with limited success. (AIDS, cancer, and malaria provide sobering examples.) Improvements to our manufacturing and other responsive capabilities should come more readily but will require more leadership and commitment than has been evidenced. Moreover, even substantial gains probably will still leave us with adaptive speeds slower than those with which pathogens can be selected and developed by terrorists. It seems evident, though, that the gains from such a program would be (a) likely; (b) worth much more than their cost; (c) of notably higher value than the rewards from pursuing specific pathogen targets to the point of licensure; and (d) better adapted to the problem that confronts us.

---

[171] U.S. Army Materiel Command, Broad Agency Announcement, Solicitation W911NF05R0011 (August 22, 2005).

[172] Available at <http://www.darpa.mil/dso/thrust/biosci/amp.htm>.

[173] Thomas R. Cech, "Fostering Innovation and Discovery in Biomedical Research," *Journal of the American Medical Association*, 294 (September 21, 2005), 1390–1393.

CHAPTER SEVEN

Organizational Coda: The BEAT Team or Biological Council

Over the long term, how we conceive of our problems is more important than our present programmatic choices. When we misperceive our problems, we misperceive our objectives, and our tactical steps are as likely to lead us astray as to be helpful. In turn, our programmatic choices are more important than our methods of organization. Good organizational arrangements, like good roads, facilitate progress, but they are not themselves the engines of progress. As suggested in the first section of this paper, we should not mistake new committees, commissions, and departments for achievement. Accordingly, organizational commentary is the least important of the three tasks of this paper (analyzing the problem, suggesting programmatic changes, suggesting organizational innovations).

Nonetheless, it has value. If necessary, we can drive our programs off the roads, cutting cross-country to reach desired goals. But it is harder to go off-road; some organizational effort facilitates forward movement. And organizational efforts are particularly important when, as at present, we are not bringing all our relevant expertise to bear. Section VI discussed one such difficulty in the intelligence community and recommended a Case X committee to deal with it. This section returns to the broader problem of developing a strategy to counter bioterrorism across our professional, bureaucratic, and interest group perspectives. It recommends a more comprehensive organizational step in addition to the Case X committee.

It is unfortunate that the number of experts with policymaking perspectives on bioterrorism within the government and the number of biologists, doctors, and other professionals advising the government at high levels total fewer than a hundred people. The benefit of this misfortune, however, is that the group is small enough to permit informal methods of discussion and coordination. Moreover, though these leaders are not without instances of turf consciousness, ego, and appropriately rooted differences in points of view, they are, as a general rule, talented, dedicated, and disposed to working with one another.

The biggest difficulty in any group enterprise, and especially in a relatively new undertaking, is arriving at a common agenda and working across bureaucratic and professional boundaries (the "seams" of the problem). The best corrective for this difficulty in the case of bioterrorism would be to bring the group of experts together frequently[174]—to discuss common issues, to evolve informal

[174] The meetings should have specific agenda items (interdiction, decontamination, etc.) but should minimize presentations and maximize time for in-depth discussion. To encourage candor, they should be off the record. To achieve this privacy while complying with the Federal Advisory Committee Act, it needs to be clear that this group is not a decisionmaking body, does not arrive at consensus recommendations, and varies in its membership from meeting to meeting.

divisions of labor and understanding of different competencies, to develop trust, and to identify topics that are being neglected.

Progress on particular issues should emerge from this effort, but the true goal—and most appropriate measure of success—is development of a common perspective, and from that a broadly shared strategic understanding about the unfamiliar problem of bioterrorism. That perspective may start with some of the views recommended in this paper, but a group process is likely to produce better insights than this individual product. As a slogan of the software industry holds, "No one is as smart as everyone."

Three meetings of this kind were conducted in 2003; the first two under the auspices of the Deputy Secretary of Defense and the third with funding from the Sloan Foundation. Each involved about fifty experts, the first two for a day each, the third for two days. Participants included the key officials concerned with bioterrorism in DHS, DOD, HHS, the FBI, and our intelligence agencies, as well as leading academics, pharmaceutical and biotech executives, and local public health officials. A core of about thirty people remained constant through the three meetings, with the other twenty varying to introduce more people into the mix and to increase the expertise on selected topics.

Unfortunately, these meetings ended as the Deputy Secretary of Defense rotated out of the Federal government and the urgency ascribed to the issue diminished in the wake of the invasion of Iraq and the failure to find weapons of mass destruction there. If, however, the premise is accepted that bioterrorism is a long-term problem and a likely vehicle of catastrophic activity, the modest funds for these meetings should be readily provided and the process reinitiated. At the urging of the author, an additional gathering funded by the Sloan Foundation has been conducted in 2007, and the Department of Homeland Security has agreed to support two further such meetings.[175] It is important to make this a continuous process.

[175] Two San Francisco Bay Area meetings and two Boston area meetings of bioterrorism experts were also conducted in 2007 on the model of the National BEAT team meetings, and the Department of Homeland Security has supported three further such meetings. Funded by the Sloan Foundation, these meetings aim to inventory local expertise, encourage collaboration between experts who are physically near one another, and better connect these experts with the national policymaking process.

CHAPTER EIGHT

Conclusion

A number of factors conspire to lead us to neglect bioterrorism. We fight our wars year by year, respond to natural emergencies day by day, and discount long-term risks; we plan for incidents and ignore the likelihood that reload will force us to cope with campaigns; we plan for larger versions of familiar, smaller events and fail to confront risks of comprehensive catastrophe; we treat natural and terrorist risks as separate things addressed often by different budgets and bureaucracies; we recognize our past failures to perceive and predict, but we respond by redoubling our efforts to perceive and predict instead of planning for surprise. Our efforts against other forms of terrorism are bedeviled by some of these failings. If bioterrorism is to be properly understood we will need to confront all of them. I hope this paper will contribute to this more realistic and broad-gauged thinking.

APPENDIX

Lidar as a Lifeline in Confronting Bioterrorism

By Richard Danzig

Efforts to use laser detection and ranging (lidar) as a means of detecting bioterror attacks have focused on the problem of alarm against bioterrorist attack. Because lidar systems cannot readily distinguish between pathogenic and natural occurrences these efforts have been found wanting. In this short presentation, I emphasize a different but important way in which lidar systems could contribute to national security against bioterrorism. By reorienting our approach, lidar could uniquely provide a solution to a neglected aspect of the bioterrorism problem. Moreover, this new approach also offers the prospect of ultimately helping to address the old, original problem of serving as a bioterrorism attack alarm.

At present, anthrax is both the dominant bioterrorism concern and the most useful simplifying example of the problem we face. Data from public assessments of the anthrax sent to Senator Tom Daschle's office in October 2001 suggest that one gram of material might contain 1×10^{12} anthrax spores, whereas 1×10^{4} is a widely accepted estimate of the lethal dose for the average person. Accordingly, theoretically, if perfectly distributed, a gram of this material might be capable of killing millions of people.

Of course, no such efficiency could be achieved. But if an aerosol distribution (the most efficient distribution mechanism) occurred in a major urban area, more than 100,000 people might be infected. Over 90 percent of these could be expected to die if not treated with antibiotics within approximately 48 hours of exposure. The problem is compounded by the fact that an attack would likely be invisible and, as a general rule, more than 48 hours would pass before those exposed would manifest symptoms.

In this context, much of our technological effort has understandably gone into detecting an aerosol release and then initiating antibiotic treatment within 48 hours. A variety of sensor technologies are now being used for detection, but, because of false positives, lidar has been found to be inappropriate for this task. In this context, much of the lidar work has focused on making incremental progress in improving discrimination, but it has had only limited success.

A second problem has been largely neglected, but is of substantial importance. Though our present strategy aims to "detect to treat," our existing sensors and models would provide little ability

This essay stems from an invited presentation to the Second Symposium on Lidar Atmospheric Applications at the American Meteorological Society Annual Meeting in San Diego in January 2005. It will be published in the *Bulletin of the American Meteorological Society* and is reproduced here with the permission of the AMS.

I would particularly like to acknowledge my debt to Dr. Shane Mayor of the National Center for Atmospheric Research and Lt. Col.(ret.) John Carrano, formerly of DARPA's Microsystems Technology Office. Both have been exceptionally generous with their technical advice and in creating opportunities for the development of the ideas presented here. One of those opportunities was a workshop on this subject sponsored by DARPA in April of 2004. I am grateful to participants in that workshop, and particularly to Pamela Clark and Dave Ligon of the U.S. Army Research Laboratory, for their observations.

within the critical first 48 hours to determine whom to treat (and not to treat, an equally important problem given limited supplies, some risks from treatment and the need for public reassurance). That is, we won't know where an aerosol cloud has propagated. This is because our systems are composed of a limited number of point sensors that indicate only whether a cloud has passed over the point, not where it came from or where it was going. Using point and wind data, computer models that are likely to prove useful in a nuclear explosion or a chemical accident or sabotage cannot adequately map the path of a biological attack. A biological attack is likely to contain so many unknowns that it will make Monte Carlo simulation modeling unworkable, or at least not workable within the required timeframes. These unknowns include, most significantly: the time of attack (point samples are collected only every 24 or 12 or 6 hours; a positive response is not time-demarcated), the place of attack initiation, the agent used, the quantity of agent, the duration of attack, and whether the attack involves a point or line source. Though our understanding of urban microclimates should improve, gains in this respect and in modeling capability are not likely to overcome these deficiencies in information.

These failings in retrospective modeling place a premium on observation of clouds as they develop in an attack. My proposal is that lidar systems could be used to discern cloud initiation and transport. Four or five lidars could be operated in concert, focused at building-top levels (though also with some look-down capability). I expect that clouds of the density associated with a 1-kilo anthrax attack with material of the purity inserted in the Daschle letter could be discerned by lidar systems tuned in the 1.5 to 2 micron range. (Backscatter may optimize for particles at twice the size of the lidar wave length. An aerosol is commonly thought to best assure inhalation when it maximizes particles in the range of 2 to 5 microns in diameter.)

This observational capability would still be subject to the false positive problem. The lidars would discern not only a biological attack, but also other aerosol releases (such as fires, construction contamination, and pesticide spraying), and natural occurrences. However, the system initially could use lidar data not as an alarm mechanism but instead simply to produce mosaics (perhaps every minute) that would be archived in computers without examination. Only after an attack was signaled by our non-lidar sensors (or epidemiological indicators) would the lidar data be reviewed. Then the cloud that triggered the sensor response (or could explain the epidemic data) would be identified. This would permit a more targeted use of antibiotics through the determination of hotspots. It would also greatly facilitate demarcation of areas subject to contamination and therefore help to map exit routes and guide decisions as to resumption of normal activities. In this way, lidar, operating as a part of a suite of sensors, could make a substantial contribution to an important problem.

Beyond this, a yet more significant accomplishment could be secured by the hypothesized lidar system. The dominant problem after a first or second attack would be how to interdict future attacks. After a first attack, for this reason, the lidar system would be used differently—lidar data would now be reviewed in real time. This data would be interpreted with several advantages—the modus operandi and the cloud pattern from the prior attack would be known; some activities that generated false positives (e.g. pesticide spraying) would likely be restricted; and tolerance of false positives would be higher. In this context, when a cloud was discerned, it would produce an immediate police movement to the scene of initiation with real possibilities of interdiction. (This would be especially so if, as seems probable, an attacker used the same modus operandi as previously and sprayed for a number of minutes.) This lidar system would thus offer our first opportunity to develop a method of interdiction to prevent future attacks.

If lidar were used to address the first two challenges, it would also begin to present options for dealing with the traditional problem of warning in the context of repeat attacks. With a pattern in mind and a higher tolerance of false positives, lidar detection of a suspicious cloud initiation would

and could be used for downwind warning. I believe the experience atmospheric scientists have gained using lidar to warn of tornadoes is valuable not only in the sensor technology but also in the insight it has provided as to how to convert lidar data into warnings on which citizens could act.

Two Federal programs are relevant to the development of such a system. The first, in the Department of Homeland Security, Office of Science and Technology, is contracting for mathematical and other simulations to ascertain the extent to which biological attack clouds likely can be discerned (and for how long) by lidar systems. The second, undertaken by the Department of Defense, is currently testing both Doppler and REAL lidars. I encourage readers working in the lidar area to contribute their skills to address national security issues generally and this one in particular.