

PART I

THE CHALLENGE OF BIOLOGICAL TERRORISM

INTRODUCTION

Over the last several years, a confluence of events – the World Trade Center bombing, the Tokyo subway sarin gas attack by the Aum Shinrikyo, and the bombing of the Murrah Federal Building in Oklahoma City – focused attention on the growing threat of terrorist use of chemical, biological, radiological, or nuclear (CBRN) weapons in the United States. These developments gave rise to a set of perceptions – among policy makers and the public alike – that the United States is vulnerable to terrorist attack; that such attacks could entail the use of CBRN weapons; and that the United States has not been well prepared to deal effectively with such a challenge.

This set of perceptions promoted a sense of urgency among lawmakers and other policy makers that the United States must act. Over the last five years, the U.S. Congress has provided substantial financial support to many government agencies that have initiated programs to address the CBRN terrorism problem.

The rapid emergence of the perceived threat and the urgency of the U.S. government's response did not provide an opportunity for full development of a systematic analysis of the CBRN terrorism problem. In particular, programs were begun without a strategic framework to guide program definition and resource allocation. Such a framework can serve several critical functions: defining objectives and relating means to ends; identifying key functions of an effective response; creating awareness of tradeoffs among those key components; determining their priorities; and establishing the basis for sustained support of the most critical components over time.

The need for a strategic framework to address the threat of terrorist use of biological weapons (BW) is especially critical. Biological weapons unique instruments of violence, and many of their characteristics could make them particularly attractive for terrorists contemplating the use of mass casualty weapons. As a result, biological weapons could become the mass casualty weapon of choice among terrorists in the years ahead.

Terrorist use of biological weapons could produce widespread, devastating, and tragic consequences. According to the Office of Technology Assessment, if used under optimal conditions, biological weapons could have an impact similar to that of a small nuclear device. A single attack using a sophisticated biological weapons in a major metropolitan area such as Washington, DC could kill as many as 3 million people. Even if casualty levels from a biological attack do not achieve their theoretical maximum, *any* terrorist use of biological weapons in the United States could have profound effects.

Bioterrorism differs from other types of CBRN terrorism in that it would impose particularly heavy demands on the nation's public health and health care systems. Although a chemical attack would also tax these systems, bioterrorism would impose especially stressful burdens. Yet, that same public health system is *the* crucial factor in an effective response. A highly effective public health system should make an important contribution to deterring the threat by demonstrably diminishing the gains of a potential attack. It also constitutes the "first line of defense" in the event deterrence or prevention fails. Ultimately, it will be the public health system that will be called on to mitigate and ameliorate the consequences of a bioterrorist attack.

A number of programs are underway to improve the health and medical dimensions of the national response to the threat of bioterrorism. Uncertainty exists, however, as to whether current programs are those that are most needed or whether they are being implemented in the most effective way possible. This uncertainty exists because to date there have been insufficient means to judge the efficacy of existing programs. This lack of criteria is the product of not having an analytic framework that establishes national requirements for an effective response derived from a comprehensive threat assessment. The development and application of a strategic framework is urgently needed. Making a contribution to the development of that framework is the purpose of this project.

This report analyzes the requirements for an effective health and medical component of the overall bioterrorism response system and assesses where the United

States stands today in meeting those requirements. It does so in the context of an evaluation of the current bioterrorism threat. What is the link between the two? It is simple: a better and more sophisticated understanding of the threat – which emerges from this analysis as a complex, multidimensional phenomenon – better informs decisions about needed response capabilities, helps establish priorities, and more effectively guides resource allocations. The report also includes a series of recommendations, both general and specific, that could strengthen current and future health and medical response capabilities.

Shortcomings of Vulnerability Assessments

One might ask why there is a need for such a study, given that several analyses of terrorism with biological weapons have already been conducted. The reason is that most of the studies done in relation to health and medical requirements of a response to bioterrorism have focused on what biological weapons *could* do, not on what they are most likely to do. They are vulnerability assessments, which, as suggested by terrorism expert Brian Jenkins, suffer from a number of drawbacks in guiding policy and establishing resource priorities.

First, the vulnerabilities of the United States to a bioterrorism attack are virtually infinite. As a result, no definitive catalogue of problems can be developed against which to plan and allocate resources. Defining the bioterrorism problem as virtually limitless can also instill policy paralysis. Confronted with an enormous range of potential disasters, it is hard for policy makers and those who lead response efforts to know where to begin.

Second, vulnerability assessments lead to worst-case analysis. Emphasizing vulnerabilities promotes a focus on catastrophic events, regardless of their likelihood. Indeed, as terrorism expert Brian Jenkins argues, “focusing on only the most horrendous events overwhelms any estimates of their likelihood. The possibility of occurrence becomes irrelevant unless the threat can be dismissed with a high degree of confidence –

of course, it cannot.” In fact, the possibility of occurrence, the likelihood, of an event is a critically important factor in planning efforts. It does little good to engage in elaborate preparations for an event that is not likely to happen to the exclusion of addressing those contingencies that are. Moreover, as the Gilmore Commission and others have argued, the assumption that lower consequence/higher probability events can be treated as “lesser included cases” of more catastrophic contingencies is not necessarily warranted.

Worst-case analysis, therefore, can skew resource allocation. It can shift limited resources – money, manpower, and time – toward high consequence, low probability events and away from those events that are lower consequence, but higher probability. The danger, of course, is that without proper preparation, even so-called “lower consequence events” could produce results with significant impact both locally and nationally.

Third, vulnerability assessments create a mentality that tends to reify “what ifs” into imminent risks. In the way that high consequence scenarios are discussed and approached, theoretical possibilities are too often transformed into real contingencies. The result is to give such possibilities more credence than they deserve.

Vulnerability assessments, therefore, while identifying the potential scope of the challenge, provide no sense of whether or not those vulnerabilities can and will be exploited by a terrorist. As a result, they can produce a misdirected planning process, inadequately defined policy choices, and distorted resource allocations.

Vulnerability assessments, however, are not without value. It is natural for policy makers and lead responders to focus on vulnerabilities and the high, indeed catastrophic consequences that could ensue if theoretical possibilities did become reality. No policy maker could accept ignoring the possibility of such consequences even if they were highly unlikely. To do so is politically unacceptable. Vulnerability assessments, therefore, identify contingencies that, while perhaps not central to the planning process,

nevertheless constitute possibilities against which some “hedging” is necessary so that, if the unlikely happens, the system is not totally unprepared.

An effective response to the bioterrorism threat, then, includes both threat and vulnerability assessments – the former to determine the most plausible threat against which the majority of planning and resources should be directed, and the latter to identify those outcomes whose consequences are so severe that they demand some preparatory action and some resources. Of course, what the balance will be between core planning and hedging and how resources will be divided among them is often hard to determine.

The Need for a Strategic Approach

Successfully meeting the challenge of bioterrorism requires a multifaceted response. No single approach will, in and of itself, be successful. It must also be a response that is *strategic* in nature. Clausewitz defined strategy at the military level as “the combination of individual engagements to attain the goal of the campaign...[It is] the employment of battles as a means to gain the object of war.” At the level of national policy, a strategy is the intellectual construct that marshals all appropriate resources and guides them toward the achievement of the objective. For the response to bioterrorism to be genuinely strategic, it must integrate all critical policy tools in an approach in which those elements of policy are mutually reinforcing, support the same objectives, do not work at cross purposes, and provide a flexibility that is responsive to changing circumstances and different conditions.

A strategic response to the BW terrorism challenge, therefore, is one in which:

- Each element of policy is as strong as possible.
- Those elements of policy are brought together in a framework marked by
 - ❑ Clearly defined objectives;
 - ❑ Awareness of pitfalls and potential contradictions; and

- Emphasis on reinforcing strengths of individual policy tools and compensating for shortcomings.
- The U.S. government is organized to facilitate strategic thinking and action, including
 - Mechanisms for the effective exchange of information and interaction of key players; and
 - Flexibility and responsiveness to change.

The Need for Flexible Response

This report emphasizes the need for a strategic approach to the development of public health and medical response capabilities. It places particular emphasis on the need for flexibility. To be successful, any strategy must be agile; it must be flexible enough to adapt to the full range of potential contingencies that can cause harm.

Strategic flexibility derives, most importantly, from having more than a single response option that allows for tailoring responses to the specifics of the event and the severity of the crisis. It diminishes the prospect of wasting resources by not incorporating elements that are marginal or irrelevant to the challenge at hand. Furthermore, it improves the chances of avoiding unintended consequences.

In the military realm, an analogy that provides important insights is the evolution of NATO strategy. In the late 1960s, NATO shifted from a strategy of massive retaliation to a strategy of flexible response. It did so because the alliance did not want to depend on the threat of a major nuclear retaliation as its only response to a wide range of potential contingencies, from a limited “land grab” by Warsaw Pact forces to their full-scale invasion of Western Europe using conventional forces alone. The catastrophic scenario, a strategic nuclear attack by the Soviet Union against the United States or Western Europe – the “bolt out of the blue” – was one for which the threat of massive retaliation was deemed appropriate. But it was also considered highly unlikely. For those events considered more likely but of lesser consequence, the implications of only having the ability to respond with a major nuclear attack were not acceptable to alliance

political leaders. As a consequence they improved NATO's "front-end" capabilities, particularly allied conventional forces. If those capabilities proved insufficient, then NATO would move to ever more dramatic options to deal with an escalating crisis. In essence, NATO strategy came to depend on having a range of effective potential options that could be applied in ways appropriate to the crisis at hand.

The NATO experience suggests a number of lessons for developing a strategic response to the threat of bioterrorism. First, a single, massive response option has serious drawbacks with respect to both resource allocations and unintended consequences. If the only response available to a bioterrorism incident – particularly those that are most likely but of consequences below catastrophic levels – is mobilization of a massive federal apparatus, resources may be unnecessarily expended because more limited capabilities, perhaps local resources augmented in selected areas, are all that are needed to deal with the problem. Moreover, such a massive mobilization could create unnecessary public panic, media scrutiny, and political repercussions. A strategic response should be viewed as drawing on a spectrum of capabilities that can be tailored to the event, organized to be implemented in a phased or tiered manner in increasingly demanding circumstances.

Second, along this spectrum, enhancing "front end" capabilities – surveillance, detection, and assessment – is likely to yield disproportionate dividends. The better the deployed initial capabilities are to meet the crisis, the less likely the crisis will escalate. In the bioterrorism context, this "lesson" suggests paying special attention to improving surveillance and epidemiological capabilities as much as possible. Robust surveillance, epidemiology, and laboratory capacity could lead to fewer demands on medical treatment – and all of the tasks that entails – by limiting the number of victims.

Third, creating flexible response options is neither easy nor cheap. An effective flexible response capability creates more demanding planning requirements in that it entails the coordination of more policy areas and more actors, requires extensive and ongoing training and exercising, and can involve complex communication requirements. It depends on organizational adaptability, which is not always a hallmark of government

bureaucracies. A flexible response strategy also relies on high levels of cooperation among a range of independent actors, which is not always easy to promote. Moreover, it absorbs significant resources in an effort that must be sustained over time. Shifting to Flexible Response was expensive for NATO because developing effective conventional forces was costlier than relying on a limited arsenal of nuclear weapons. Similarly, implementing an effective flexible response strategy to deal with bioterrorism could entail significant expenditures over time. The alternative is to rely on a limited number of response options that may or may not be appropriate to the specifics of a crisis and that may or may not provide the right kinds of hedges against the less likely but potentially catastrophic contingencies.

This report addresses these issues and provides recommendations on means by which the U.S. government can enhance its strategic approach to improving the health and medical dimensions of the response to the challenge of bioterrorism. The recommendations are offered as a contribution to promoting effective national responses to a challenge that deserves sustained attention, adequate resources, and unflinching political will.

THE BIOLOGICAL TERRORISM THREAT: A MULTI-FACTOR ASSESSMENT

Introduction

Biological agents are living organisms, or the byproducts of living organisms, that cause diseases that lead to incapacitation or death. The most pervasive characteristic of the threat of terrorist use of such biological agents is its uncertainty. An enormous range of possibilities exists in terms of the character and impact of a bioterrorism attack; the variety of scenarios that could be elaborated is virtually unlimited. Anything can happen. Popular culture is suggestive in this regard. It has produced movies and books using bioterrorism as their major plot device, describing situations from a lone scientist genetically modifying diseases to strike against major urban populations to fanatic ethno-separatist or religious groups exploiting agents that have been researched for biological warfare to hold cities or governments hostage.

These fictional accounts, however, may be divorced from reality, and they may have contributed to fostering an impression of biological terrorism as easy and effective that does not square with the facts. With respect to biological terrorism, the formulation that “it is not a matter of if, but when,” also is not helpful. Something may never happen. The historical incidence of successful biological terrorism is very, very small, and, while the past is not always prologue, history should not be ignored. With respect to the threat, therefore, we just do not know with any certainty.

A threat assessment is needed precisely to reduce the uncertainty that currently permeates the debate over bioterrorism. Undertaking a threat assessment is particularly important in the current environment in which government investments in programs to combat terrorism with chemical, biological, radiological, and nuclear (CBRN) weapons are increasing significantly. We will be able to ensure that society is prepared in the event of a bioterrorism incident – and to do so in a way that ensures that taxpayers’ money is wisely spent – only if the nature of the threat is systematically addressed, and its complexity is understood and appreciated.

A good threat assessment will create a “threat envelope” that describes the most plausible contingencies and identifies those possibilities that fall within it and those that lie outside. Defining a plausible threat envelope also provides a means to identify those contingencies that require hedging, in that, due to the severity or enormity of their consequences, some preparation for them should be undertaken, even if they are relatively unlikely. The combination of the threat envelope and the hedging contingencies should give policy makers some measure for making decisions regarding policy priorities and resource allocations.

A framework is needed for thinking about the bioterrorism threat. That framework should cast the threat more in the nature of a forecast than a prediction; that is, it should identify the ranges of probability of something happening, while recognizing that those ranges can sometimes be quite wide. Expecting certainty creates a standard that will never be achieved, and it implies a greater precision in the analysis than, in fact, can be achieved given the complexity of the subject matter.

An analytical framework for thinking about the biological terrorism threat will also highlight the fact that the threat is not unidimensional; it does not come from only one factor. Rather, it is composed of several elements. For purposes of this study, the key elements of the bioterrorism threat have been identified as the *who* (the actor), the *what* (the agent), the *where* (the target), and the *how* (the mode of attack). Each of these elements, in turn, entails a significant array of possibilities. The different kinds of actors who might try to exploit biological weapons, the large number of potential agents, and the variety of possible dissemination methods are some examples of the complexity of each element of the threat. The endless scenarios and contingencies that have been described as potential bioterrorism events represent the plausible or fanciful combination of the many facets of these factors into particular configurations.

The key to a successful bioterrorism threat assessment, therefore, is disaggregating the threat into its component elements and assessing the relationships among them. Only by doing so can one examine comparative likelihood of various

contingencies. With the ability to make those comparisons, policy makers will have a better means by which to determine those contingencies that are more important. It is the introduction of likelihood into the analysis that distinguishes a threat assessment from a vulnerability assessment, a distinction of critical importance, as already discussed.

The goal of this assessment, then, is not to provide a detailed examination of every possible bioterrorism scenario or contingency, but to suggest an analytical framework about the biological terrorism threat that facilitates making judgments about effective responses – especially in the public health and medical arena.

In the last several years, the analytical community has given considerable attention to the bioterrorism threat. This assessment is not intended to “reinvent the wheel” by replicating these existing studies, but to take the best of that work and integrate it into a coherent, holistic framework. The bibliography on which the project team drew and the experts interviewed for this phase of the project are presented in the appendix.

Integrating the Components

The key components of the threat assessment – who, what, how, and where – must be pulled together into an integrated assessment that provides the basis for formulating policy and program requirements for an effective national response. The analysis that constitutes such an integration, however, must be informed by several important considerations.

The Impact of Change

In looking to the future of the threat of biological terrorism, three sets of changes are especially important to note: technological change, the changing socio-political context, and the changing face of terrorism.

Changing technology will have an impact on future terrorist options. People have described the next hundred years as the “century of biology,” and incredibly rapid and profound changes in biotechnology in particular are likely to have a major influence on the prospects for bioterrorism. Genetic modification, biomolecular engineering, and enhanced bioproduction technologies, for example, may make it easier for terrorists to overcome the barriers that inhibited acquisition of biological weapons in the past. Technological change, however, should not be considered only for what it might do to make the threat more severe, but such change must also be evaluated for what it can do to facilitate responses to the threat. Advances in biotechnology and materials sciences, for example, may underpin the development of rapid and effective detection and identification devices. Breakthroughs in understanding of human physiology may provide new approaches to improving the immune response to pathogens. Evaluating the future terrorism threat demands that we pay attention to both positive and negative aspects. It requires a balanced appreciation of the impact of technology, not just a focus on what may capture the headlines.

Technological change is only one aspect of the evolving context within which the new terrorism will have to be confronted. That context involves the interplay of political, economic, social, ethnic, and religious factors, not just in one country but around the world. The terrorism of the future will be in response to broad trends such as globalization, accelerating interconnectedness, and population dynamics, but it is also likely to entail narrow psychological elements from marginalization to techno-rage to revenge for real or imagined wrongs. As motivations move away from the traditionally political, the more important the special mindsets of potential terrorists become. Refining understanding of the threat of bioterrorism demands special attention to these distinctive mental topographies. Equally important is the requirement to understand how these unique psychologies interact with circumstances, capabilities, and opportunities, to take potential terrorists down particular paths, including one path (among many) at the end of which may be the use of biological weapons.

A third aspect of the evolving environment is the changing face of terrorism itself. In part, it is a question of the change in the actors. Of the current watch list maintained by the U.S. Department of State of terrorist groups of concern to the United States, more than half were not on the list at the end of the Cold War. The structure of terrorist actors, however, is also changing, as more transnational, network-based entities join traditional organizational hierarchies, a development exemplified by Osama bin Laden's al-Qaeda. Terrorist tactics also appear to be evolving, with more indiscriminate attacks and less acceptance of responsibility for those attacks that do occur.

“Lessons” of History?

Finally, much of the skepticism about the severity of the bioterrorism threat derives from the fact that, historically, not only have few terrorist attacks with biological weapon been attempted, but those few that can be identified have either been unsuccessful or have produced only limited results with respect to casualties. Looking to history for answers to the bioterrorism threat, however, provides mixed results. This is the case for several reasons. First, the historical record in fact identifies relatively few data points, especially with respect to BW use. Second, while developments in the years ahead must be expected to combine continuity and change, which one will dominate? It is not necessarily the case that, in all things, the future will resemble the past. History provides few precedents, clear indicators, or discernable trends to instill confidence that looking at history will alert us in advance to what will happen in the future, particularly given the nature of the changes mentioned above and the variety of factors involved in shaping the bioterrorism threat.

Evaluating Bioterrorism “Pathways”

The project team used a “matrix-pathways” approach to integrate the components – actor, agent, method of attack, and target – into a representation of the complex nature of the bioterrorism threat. Given the importance of the actor in shaping the threat, the team decided to break the question of “who?” into two distinct but related elements

suggested by the questions: “what are the motivations for a group to use a biological weapon?” and “what capabilities must an actor possess to develop and use a biological weapon?” These five components provided the starting point for constructing the matrix. This matrix is represented graphically in Figure 1.

A bioterrorism pathway is produced by systematically identifying plausible relationships between factors and outcomes. For example, a group seeking to produce over 500 casualties will need certain connections between its internal group dynamics, technical expertise, dissemination technique, and target to reach its desired goal. Working

Motivation		Capabilities			Agents			Dissemination		Target	
Number of Casualties	Level of Panic	Group Size	Technical Proficiency	Financial Resources (x \$1000)	Agent Availability	Ease of Growth	Morbidity and Mortality	Ease of Dissemination	Efficacy of Dissemination Technique	Number Exposed at Target (x 1000)	Target Vulnerability
50000	High	1000	Expert	1000	High	High	High	High	High	1000	High
5000	Med.	100	Good	100	Med.	Med.	Med.	Med.	Med.	100	Med
500	Low	10	Low	10	Low	Low	Low	Low	Low	10	Low
50	Low	Loner	None	1	None	Low	None	Low	Low	1	None

Figure 1 – Bioterrorism Pathways Matrix

through the complete set of factors generates a bioterrorism pathway. In many cases, a pathway cannot be completed because logical connections between factors and desired outcomes cannot be made. For example, a group seeking to create disruption or illness without actually killing anyone is not likely to follow the path of an aerosolized anthrax attack. Using the threat matrix in this way produced the set of possible bioterrorism pathways. Combining these pathways with judgments regarding the comparative likelihood of each pathway produced the “plausible threat envelope” for bioterrorism.

Some examples of pathways are represented graphically in Figures 2 and 3. The first example represents a pathway that successfully produces a middle range attack using anthrax that infects a total of 500 people. The second example has two variants in which an attempt to produce a mass casualty anthrax attack (over 5000 people infected) ultimately fails. In the red variant, the group plans to carry out numerous small aerosol releases of anthrax slurry in a large metropolitan city. The attack fails due to a lack of microbiological expertise within the group. The group possesses the resources to illicitly acquire a sample of anthrax, a large fermenter (500 L), and sufficient quantities of growth media. However, the type of growth media obtained is not ideal for growing anthrax and the particular strain of anthrax does not grow rapidly. The group is consequently not able

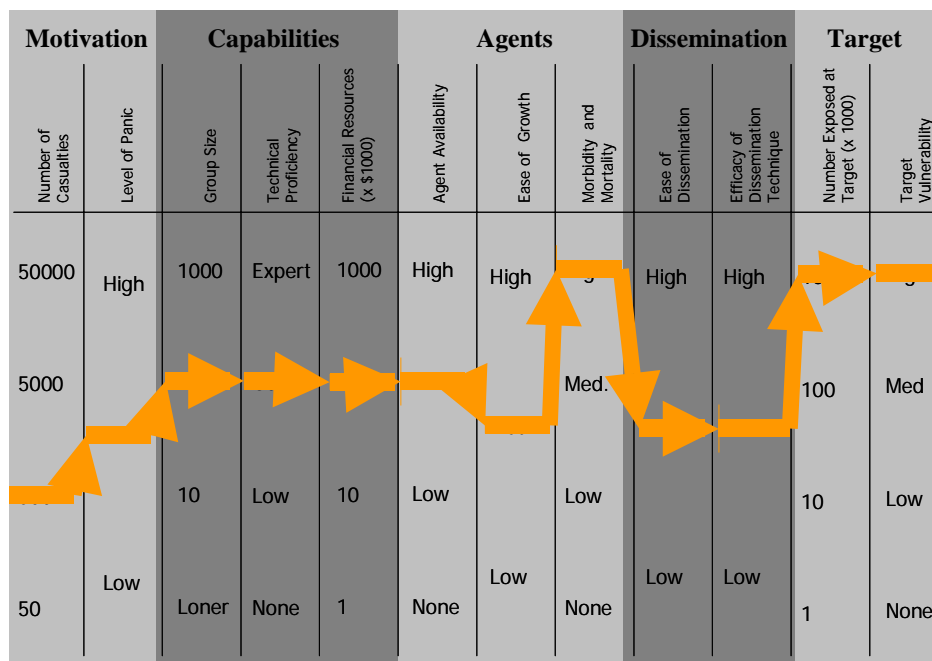


Figure 2 – Successful Mid-Range Attack (500 Casualties)

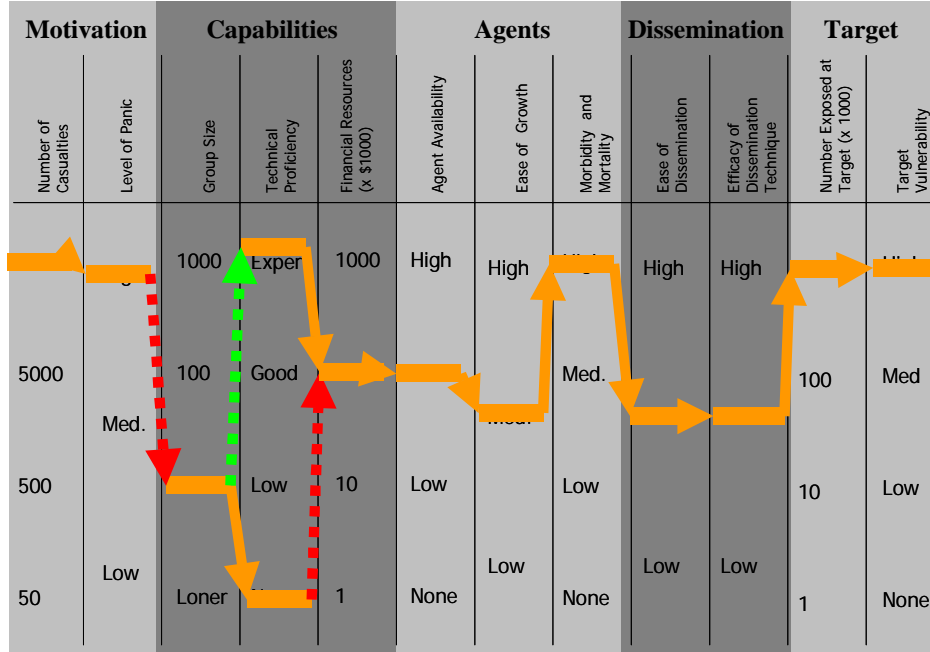


Figure 3 – Failed Attempt at Mass Casualty Attack

to produce sufficient quantities of viable anthrax slurry to execute a successful attack. The green variant of this example shows that the group, while possessing many of the technical requirements, is not large enough to enjoy the full set of skills necessary to conduct a successful attack.

These two examples are hypothetical. The project team also examined the historical record to inform its pathways analysis. It did so in two ways. First, it examined cases of bioterrorism to determine the pathway that was exploited. Figure 4 represents the case of Aum Shinrikyo which, despite having a large manpower pool, scientific expertise, major financial resources, technical equipment and so on, was nevertheless unsuccessful in conducting several biological attacks aimed at producing large casualties because it did not have the appropriate agent. Figure 5 represents the case of the Rajneeshee cult in which the motivation to achieve a limited impact through

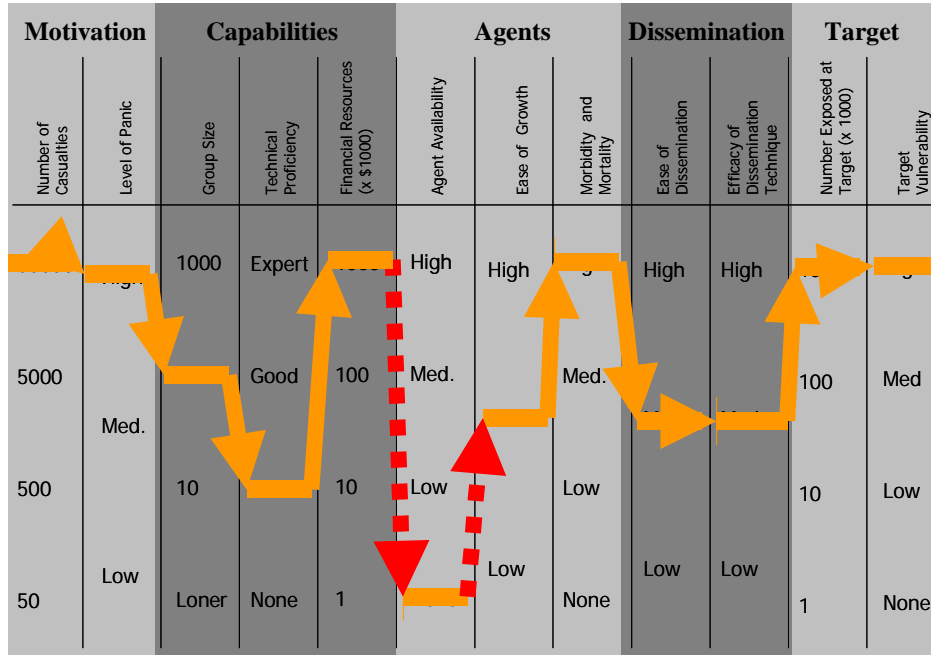


Figure 4 – Aum Shinrikyo’s Failed Catastrophic Attack

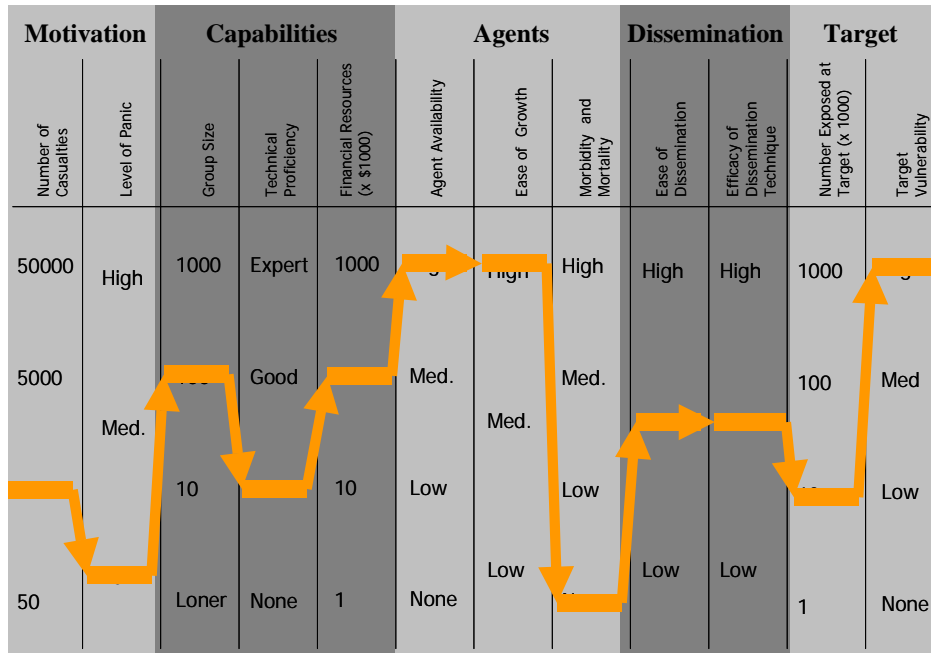


Figure 5 – Rajneeshees Attack in Oregon

the use of biological materials produced a less sophisticated, but ultimately successful pathway.

Second, the project team turned the question around and asked whether the historical record could offer analogs to some of the pathways deemed more probable than others by the project team because of the logical relationship between factors and outcomes. Given the paucity of historical data, however, this step in the analysis had limited utility.

The Threat of Biological Terrorism: Key Findings

The application of the “pathways” methodology yielded several important findings that should inform efforts to develop an effective health and medical dimension to the nation’s overall capabilities to respond to bioterrorism.

A key relationship exists between the degree of risk and the level of casualties desired in an attack. That relationship, however, is *not* the straightforward one that higher risk is associated with catastrophic casualty scenarios. Indeed, the degree of risk declines as the level of desired casualties increases, insofar as *it becomes less likely*.

In essence, *as a terrorist seeks higher casualties, fewer pathways are available to achieve that objective, and those that remain are more difficult*. There are several reasons:

- Few terrorist actors have the necessary combination of size, resources, skills, facilitative ethos (e.g., willingness to experiment and accept failure), or appropriate organizational structure to achieve mass casualty capabilities.
- Traditional agents capable of inflicting mass casualties are either difficult to acquire, cultivate and produce, or disseminate effectively. The relationship between agent and dissemination technique is especially important in that if the dissemination process is less than optimal (due to the device, the method, or the

environment), the terrorist must compensate through meeting more demanding technical requirements such as producing greater volumes or better quality agent to achieve the same effect. Producing and disseminating more agent also increases the possibility of detection and capture.

- Likely targets for bioterrorism attacks do not necessarily facilitate mass casualty outcomes given the other requirements for conducting an effective attack against such targets, including technical knowledge (of air flows in large arenas, for example) or operational skills (surveillance, planning, finance, etc.).

Despite the low probability of catastrophic bioterrorism, there is still ample cause for concern. We do not know how “massive” a mass attack has to be; worst-case scenarios may not need to happen.

Bioterrorism attacks that produce levels of casualties below those considered catastrophic constitute a significant problem for two key reasons:

- We do not know at what point the response system will become overburdened and stressed to the point of collapse. Some officials involved in response preparation, particularly at the local level, suggest that the threshold is not very high.
- Use of unconventional terrorism for other than massively destructive purposes is consistent with the historical record, which suggests that such events have often been designed to achieve more discriminate goals, including assassination and financial gain.

The danger and harm inherent in the bioterrorism threat is not limited to physical fatalities and casualties. Psychological impact and social disruption could also be severe if effective preparations are not made and useful responses are not developed.

Terrorism expert Brian Jenkins has argued that “Frightening millions may exceed the desire to kill thousands.” Terrorists might seek leverage and advantage from provoking a number of psychological reactions to even limited use of bioterrorism: panic that would magnify the attack; hysteria that would stimulate untoward behavior among the population; futility that could create momentum for responding to terrorist demands; depression that could make it more difficult to shape an effective strategic reaction; lack of confidence in government that would be seen as incapable of meeting its fundamental purpose of safeguarding its citizenry. One could argue that the Aum Shinrikyo attack, while a failure in terms of achieving mass casualties, nevertheless had a profound impact on the way we look at the world and the problems society now confronts. Targets may be selected, therefore, more for their symbolic value than for the number of people that can be killed.

Beyond the psychological impact, even a lower scale bioterrorist attack could disrupt civil society on a significant scale, both in the locale of the attack and more broadly. Experience with natural disasters or conventional terrorist attacks suggests that it could take a community considerable time for its life to return to some kind of “normalcy.”

Although many terrorists either will not be interested in using biological weapons or not able to do so, two categories of non-state actors – those with relationships with national governments and those outside the traditional scope of governmental scrutiny – warrant particular attention.

Terrorism analysis tends to exclude violent acts by non-state actors allied with foreign governments in times of conflict because such actions are considered acts of war. In terms of national bioterrorism response planning, this is short-sighted for three reasons:

- The consequences of such an attack would be no different than if it occurred as an isolated incident and the response needs would be the same.

- State-sponsored terrorists are among the few actors who could assemble the requisite resources, skills, and materials to conduct a successful attack that produces significant levels of casualties.
- Countries who see themselves potentially in a conflict with the United States are demonstrating an increasing interest in “asymmetric strategies” to obviate the overwhelming U.S. advantage in conventional military power. When combined with a perception of the United States as a country that insists on “casualty-free” conflicts, enjoys only limited credibility in terms of its commitments to friends and allies overseas, and retains little consensus on when and how to use its military power, the appeal of asymmetric strategies that include terrorism with unconventional weapons could increase.

This is not to argue that an adversary of the United States would share biological weapons technology with a non-state actor or allow such an entity to “set off” a biological weapon in isolation from a major confrontation. The potential costs will generally prevent those countries from giving the United States “a poke in the eye with a sharp stick” just for the sake of doing so. But the United States should not expect that its future will be free of conflict with adversaries in other parts of the world, and if that conflict entails interests great enough for the other party – for example, regime survival – they may be willing to “bring the conflict home” to the United States through domestic attacks by non-state actors using unconventional means.

The second category of actor that bears particular attention includes those who may not have been a regular focus of scrutiny either because they are new to the scene or they have not been considered part of the terrorism universe. Among the actors who now define contemporary terrorism – which itself is a combination of old and new dimensions – recent analysis suggests that those who might be most attracted to the use of biological agents include

- non-state actors inspired by religious ideals;
- groups from the Right of the political spectrum;
- actors with millennial world views that combine with notions of the “cleansing” value of violence;
- transnational networks that are less constrained by central authority; and
- radical single-issue groups.

Few of these actors will have the requisite skills to perpetrate bioterrorist attacks that produce catastrophic casualties. Cults, for example, tend to be insular, paranoid, smaller groups that lack the full range of skills necessary to carry out a mass attack. The diffusion of transnational networks could make it hard for them to assemble all of the necessary requirements. The concept of “leaderless resistance” that is a value of the right-wing in the United States may leave it without the organizational discipline to conduct successful attacks. Despite all of these shortcomings, however, these groups must continue to be of concern regarding future bioterrorism, if only because smaller-scale events in terms of casualties could still produce significant negative impacts.

The environment of uncertainty surrounding bioterrorism will remain.

The threat is not static and will continue to evolve. Changing actors and evolving technology – especially in biology-related areas – will be major drivers of such change but not the only ones. Globalization and the Information Revolution will shape the terrorism environment just as they will most other forms of social organization and interaction. Specific events outside the bioterrorism realm will intrude to influence terrorists’ goals, perceptions, and modes of operation. The impact of individual personalities should not be discounted.

Two points in relation to the uncertainty about the bioterrorism threat by ongoing change are important for those who must respond to the challenge. First, the assumption is usually made that such change will make the threat more severe. Such an assumption is not necessarily warranted. Change should also benefit those who must respond to the threat, not only in the tools they could have available, but in terms of the broader social, political, and psychological context. Whether terrorism waxes or wanes at any particular

time depends on a confluence of factors that is not always in the terrorist's favor. Part of the overall objective of those responsible for dealing with terrorism must be to promote an environment in which the elements that support or facilitate terrorism find expression difficult.

Second, uncertainty is created by the constant adjustment in the dynamic between terrorists and those who fight them. Like the offense-defense relationship in military affairs, the relationship between terrorists and responders is constantly in flux, and uncertainty arises because it is not possible to state precisely at any given point in time how the balance stands between them. The important point, however, is that both elements are necessary to create that dynamic relationship. In the case of responding to the threat of bioterrorism, certainty will only be achieved if we take ourselves out of the game and do nothing. In that case, we can be confident that the terrorists will prevail. Otherwise, a measure of threat and a degree of risk must be accepted. The challenge is to reduce that risk to manageable, and acceptable, levels. In the case of bioterrorism, the health and medical dimension of the overall response system will play an important role in achieving that objective.