BIOTERROR
IN THE 21ST CENTURY

Emerging Threats in a New Global Environment

Daniel M. Gerstein

NAVAL INSTITUTE PRESS
Annapolis, Maryland

Naval Institute Press
291 Wood Road
Annapolis, MD 21402

Library of Congress Cataloging-in-Publication Data
Gerstein, Daniel M., 1958-
Bioterror in the 21st century / Daniel M. Gerstein.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-59114-312-3 (alk. paper) — ISBN 978-1-59114-313-0 ((pbk.) : alk. paper) 1. Bioterrorism. I. Title. II. Title: Bioterror in the twenty-first century.
HV6433.3.G47 2009
363.325'3—dc22
2009025842

Printed in the United States of America on acid-free paper

14 13 12 11 10 09 9 8 7 6 5 4 3 2
First printing

CHAPTER FOUR

Examination of the Potential for a Bioterror Attack

> The distance between the capacity of a terrorist group to conduct a biological attack and the nation's preparedness for such an attack is widening. . . . [There is a] growing complacency in national security circles, the government, and the public mind . . . and the exponential growth of emerging, dual-use technology in biological and medical science is making the situation much more dangerous than in the past. There are reasons to believe terrorists plan to conduct an attack on the United States.
>
> Margaret Hamburg, Former Assistant Secretary for Planning and Evaluation at the HHS speaking at the Center for National Policy[1]

Overview

The potential for a bioterror attack relates directly to the critical nexus we have identified between globalization, terrorism, and biotechnology. As a result of these relationships, we find a world in which all indicators individually and collectively point to the increased capacity for terrorists to develop and use biological weapons in support of their objectives. As described in earlier chapters, prolific writings and discussion on these topics have resulted in little universal agreement as to what the future holds. Some see globalization as inevitable and a benefit to humankind. Others see globalization, or at least portions of it, as a negative force. Still others postulate a retrenchment away from globalization as a possible global outcome as they recognize the downsides of a globalized world on their insular nations, societies, and cultures.

Biotechnology is most often seen as improving the quality of life around the world, yet there is a dark side here as well on which many experts report and over which they express grave concerns. A significant tension

exists between medical professionals looking to advance biotechnology for the sake of humankind and those saying that these advances represent a form of dangerous proliferation that must be controlled. However, even those that support controlling the proliferation of these capabilities recognize, in the same breath, the challenges associated with such a position. What does the future hold for a field experiencing 400 percent annual increases in capacity? Is that growth rate sustainable? Will the rate increase even further? What about the potential for the introduction of nanobiotechnology?

Terrorism continues to be perceived as one of the most important issues facing America today, yet we cannot even agree to a definition, either nationally or internationally. It remains a highly emotional subject, with some calling terrorists murderous thugs and others rationalizing their actions. The literature tells us that where one stands on this issue is highly correlated to the target attacked and one's personal sympathies. With such a lack of clarity in understanding terrorism, attempting to address the issue becomes that much more problematic.

Turning to bioterrorism, one sees a similar lack of clarity. Many symptoms combine to make this issue perhaps one of the most difficult national security challenges we face. Even understanding the history of the issue presents challenges because previous incidents provide few definitive insights. Likewise, even with regard to the science, widespread disagreement exists concerning the potential for a bioterror attack, with some claiming the science is trivial and others claiming it is far too complex for all but the most highly trained scientists. As we begin this examination, three concerns are worthy of mention.

First, the nature of reporting on bioterror has made getting to the "truth" highly problematic. After the Amerithrax attacks, it seems as though the floodgates opened: the proliferation of articles and information about BW and, in particular, terrorist BW, has occurred at a rampant pace. However, much of this information reflects circular reporting. In other words, when one goes to the literature from books to articles to blogs, the information generally comes from a handful of key sources. The effect has been volumes of information that lead to more reporting, all based on information from just a few sources. In some cases, the sources are unconfirmed assertions. Perhaps of even greater concern is that national policy is being set based on such information. Examples can be found in of the reporting about al-Qaeda's alleged efforts to acquire WMDs that were in a listing of article compiled by CNS.[2] Several of the notes indicate that many of these allegations have not

been proven. Still, they were reported and have collectively formed some of the foundations on which we have based U.S. policy.

Second, the proliferation of technical capabilities and knowledge has likely made bioterror an inevitable part of the security landscape of the future. Scientific journals, information available on the Web, and the general information available through educational sources reflect only a subset of the potential resources available concerning biological topics, some of which would facilitate terrorists developing the capability to launch a BW attack. If you want to know what gene is thought to make the Ebola virus transparent to the immune system, you can find it in a scientific article posted on the Web. If you want to understand how to make anthrax more stable in the environment, there is a blog that can help you.

Finally, even with all the potential for proliferation of BW capabilities, the experts remain divided, with some believing a large-scale bioterror attack could be imminent, and others believing the threat is exaggerated and massive funding for biodefense detracts from other, more-pressing public health issues. Even gaining agreement on the ease with which a terrorist could develop and use BW weapons has remained a subject of intense debate. How can opinions on such a technical issue be so divergent? Which camp do we believe? And what if the camp you follow is wrong?

It is within this somewhat confused framework that we examine the nexus between globalization, terrorism, and biotechnology to gain an understanding of the potential for bioterrorist attack. We also want to understand the parameters under which a bioterror attack could become a reality. Therefore, in this chapter, we will examine four fundamental questions:

1. Will biotechnology developments make BW more readily available for terrorists in the future?
2. Have terrorists demonstrated the intent to acquire, weaponize, and use biological weapons?
3. Are the international N/CP regimes adequate to deter, dissuade, and thwart terrorists from gaining biological weapons capabilities?
4. What level of capabilities will be required to prevent and protect against terrorist BW proliferation and attack?

Before examining these complex issues, we must delve into what is meant by a bioterror attack. For this analysis, we will consider this type of attack to be one executed by a terrorist, perpetrated using biological material as the means. Additionally, we must delineate the attack into a small-scale or large-scale attack. As we will see as part of this analysis,

differences exist in requirements for perpetrating an attack based on the scale. These differences will figure prominently in our conclusions.

The author has selected the threshold of one thousand casualties with a mix of mortality and morbidity as the delineation between the two categories. Any event with 999 or fewer casualties would thus be considered a small-scale attack. However, we must realize that several important factors will go into categorizing an attack in such a way. The number "one thousand" was set above the level of the largest known modern use of BW weapons: the Rajneeshees' attack in 1984. However, the number is also set well below the 9/11 casualties that resulted in approximately three thousand deaths. In comparing the two events, the author argues that the Rajneeshee attack—with no deaths, approximately 750 sickened (with no long-term effects), using a low-pathogenic agent—would be considered a small-scale attack, while the 9/11 terrorist attacks (although they did not involve BW) with more than three thousand killed, thousands more injured, and economic losses approaching $1 trillion, would be considered a large-scale attack.

Of course, outcomes matter. The Rajneeshee attack, if it had used dried Ebola virus sprinkled on the salad bars and had affected the same 750 people, would have resulted in 90 percent primary casualties and perhaps secondary casualties of family members and health-care workers who treated the victims. The attack would thus likely have approached or perhaps even exceeded the one thousand threshold. The numbers coupled with the horrific nature of the disease would undoubtedly move this categorization into the large-scale classification, even if the threshold had not been exceeded.

The delineation of large scale versus small scale would also be based on other factors, including economic and policy implications. Incorporating these factors, a case could be made that the Amerithrax attacks had a significant effect on the United States, specifically on biodefense policy and funding, so that it should be categorized as a large-scale attack. While the policy and funding impacts are real, setting the threshold so low with fewer than ten deaths and disease in fewer than twenty-five people overstates the impact in an unhelpful way. Thus, while the economic and policy implications have been significant, they do not raise the Amerithrax attacks to the large-scale category.

Picking thresholds will always be difficult. Some will argue that any deaths due to bioterror are unacceptable. Others may argue that the numbers to date are so low they represent an acceptable loss. Placed in the context of naturally occurring disease, with 6 million casualties per year

globally to the combination of tuberculosis, malaria, and HIV/AIDS, the number "one thousand" seems almost inconsequential. However, we must balance this opinion with the concept that Jessica Stern calls "dreaded risks," which she defines as a category of risk in which the fear of an act is disproportionate to the actual outcome. She identifies BW in this category, as a means that causes fear, angst, and reactions disproportionate to the actual potential of these capabilities. The loss of confidence in government institutions were it to fail to protect the American people from BW attacks that killed one thousand would be unacceptable and intolerable.

Another delineation that will undoubtedly figure into the question of scale will be the geographic effects of the attack. BW attacks that would be geographically contained, such as those from a small amount of a noncontagious pathogen, are more likely to be categorized as small scale, assuming the number of casualties is below the threshold. However, even a relatively small release of a contagious pathogen has the potential to grow into a large-scale event if the outbreak is not identified and contained quickly. Therefore, in this case, even if the number of casualties may not reach the threshold of one thousand, it could still be considered large scale based on the greater potential of a contagious pathogen, especially if it were highly pathogenic.

This discussion implies that the delineation of a large-scale versus a small-scale attack has an element of art and cannot be reduced to a neat scientific equation. Still, the threshold of one thousand seems an appropriate dividing line from which to begin a more definitive assessment on a case-by-case basis.

The Impact of Biotechnology on Availability of BW Capabilities

This section will examine the proliferation of biological capabilities. Three components will be analyzed: (1) the steps necessary for developing a terrorist BW capability, (2) the trends in biotechnology development, and (3) the historical precedents or lack thereof concerning the use of WMDs, in particular biological weapons.

Much has been written about the threats humankind faces from terrorists' use of WMDs, with a growing body of experts claiming biological terror is becoming the most dangerous threat we face. The basic logic goes something like this: nuclear weapons, while extremely dangerous, are difficult to manufacture due to significant processing requirements, the lack of readily available fissile material, and the signature that a nuclear program produces which makes it susceptible to discovery and

elimination. Chemical weapons, while producing a fairly predictable effect and being relatively straightforward to develop, are highly inefficient due to the significant quantities of material required to achieve a large-scale outcome. Biological weapons, conversely, can be extremely potent, easily concealable, made from readily available source material and dual-use equipment, and elicit a strong psychological response among governments and victims. The detractors caution that working with biological material is not trivial and that the technical capabilities required go well beyond those of most terrorist organizations.

Required Steps for Developing a Terrorist BW Capability

We have already discussed in some detail many of the required steps for a terrorist BW program. In the subsection "Building a Terrorist BW Program" in Chapter 2, we introduced several models developed to analyze the requirements for developing a bioterror weapon. We also alluded to the inadequacy of the current models, particularly with regard to understanding terrorists' motivations. Our goal in this section, therefore, will be to develop a model that accounts for the range of capabilities and intentions that must be considered in developing a terrorist BW capability.

The OTA assessment for a state BW developmental effort provides a useful departure point for this analysis. To be useful for examining requirements for a terrorist BW program, however, it must also be adjusted for the reduced rigor and scale inherent in such an effort. So what are some of the differences?

A state planning process to incorporate a BW capability into its arsenal would have a developmental course whereby the doctrine for employment would be established determining such issues as how such a capability would fit into overall military capabilities and under what conditions such a system would be deployed. Thorough research, development, testing, and evaluation would be undertaken as well. A state would want to understand the operational parameters under which such a capability would be most effective. A logistical network would also be developed and a rotation plan established to ensure the viability of the BW material. All these steps for a state would contribute to the "fielding" a BW the capability that could be used for tasks ranging from deterrence to combat.

Additionally, the OTA includes steps and requirements that would not be relevant to a bioterrorist. The proliferation pathway described in the Congress's 1993 OTA report (see Chapter 2, this volume) articulates a formal acquisition process that exceeds the basic entry-level requirements for a small BW program. Many of the component elements such as

"develop and pilot-test production process" within the first step—R&D—have greater applicability for large-scale weapons programs. The same can be said of the "acquire individual and collective BW defense, including vaccines" in the fourth step—delivery systems acquisition. These requirements would go well beyond what might be necessary for developing and deploying a basic terrorist WMD capability.

The OTA proliferation pathway makes no attempt to address the minimum steps necessary for developing a rudimentary yet effective "terror" weapon. Just as the hijackers on 9/11 were only concerned with taking flying lessons to learn how to operate the flight controls, but expressed little interest in learning how to land the aircraft, so too could a terrorist only incorporate certain key steps of the acquisition process into his BW program.

Furthermore, while difficult to generalize the motivations of all terrorists, previous attacks have tended toward targets of opportunity designed to gain notoriety for specific causes. While some attacks have resulted in significant mass casualties such as the Africa embassy bombings and 9/11, in some regards the "battlefield" effects were less important than the psychological outcomes. This same philosophy would likely apply to deployment at a terrorist BW program where the actual capabilities would matter less than they would for a state deploying such a capability, which implies a lesser requirement for testing and even efficacy.

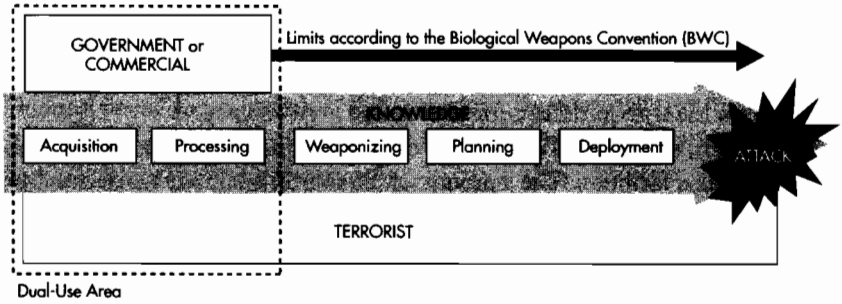
Finally, a terrorist BW program does not require extensive production and storage facilities. The amount of biological material necessary for use in an attack means that facility requirements are modest. One can certainly envision a scenario whereby the weaponized material would go directly from preparation to deployment, with no storage requirement. Additionally, terrorists have not demonstrated a desire to develop an arsenal system for storing these types of capabilities.

While terrorists have a "doctrine" of sorts, it tends to focus on achieving success in single tactical engagements. For example, al-Qaeda documents recovered from Afghanistan had material on conducting attacks and the development of BW capabilities, but did not include operational- and strategic-level doctrine for combining all their capabilities over the course of a lengthy campaign plan.[3] All these factors point toward a less stringent requirement for development of a terrorist BW program.

Given these limitations of the OTA proliferation pathway for considering terrorist BW developmental capabilities—which amounts to the overdesign of the proliferation process from the perspective of

the terrorist or substate actor—one can identify several subcomponents constituting the minimum essential steps for a BW program.

Beginning with the OTA framework and eliminating those steps beyond what a terrorist would find necessary to develop a BW capability yields a streamlined requirement consisting of five major steps (Figure 4–1). The steps account for both the capabilities and intentions that would go into preparing and executing an attack, and would include acquisition, processing, weaponizing, planning, and deployment. It is important to note each step in the model contains elements of both capabilities and intentions. For example, in the first step of acquiring the pathogen, there is the technical capability associated with gaining access to the material, growing it to acquire the necessary amount for an attack, enhancing or preparing it to have desirable characteristics, and even in knowing it will cause disease. This last bit of information is very important in dealing with biological material because even small genetic variations can yield vast differences in outcomes, as the Aum Shinrikyo cult discovered with regard to their efforts to develop an anthrax weapon.



A terrorist's ability to employ biological weapons can be represented as an engineering process with discrete components. It follows that interdicting a bioterrorist attack can be examined within the context of achieving success in any of the six phases from acquisition to attack; if the terrorist is not able to successfully execute any one of the phases, then the attack will not succeed. Throughout the process, knowledge is essential to gain appropriate materials, process and weaponize them, and finally plan and conduct an attack.

FIGURE 4–1 Steps for Developing a Terrorist's BW Capability

Figure 4–1 displays the components of a generic terrorist BW program as a systems engineering process. This is both deliberate and necessary to understanding not only how the process functions, but also what can be done to decrease the chance of a successful bioattack. To carry the systems engineering analogy to the next logical step, a successful attack is based on having the requisite knowledge and achieving success in each of the component areas or five steps. Failure across any one of the

components will result in an overall system failure. This becomes essential in understanding how to structure the U.S. homeland security doctrine to prevent, protect, respond, and recover from a BW attack. Figure 4–1 also alludes to the BWC. More on the effectiveness or lack thereof of the BWC will be discussed in a later chapter. Suffice it to say, the BWC with its inherent limitations for moderating state behavior would have even less effect on moderating terrorist behavior.

The acquisition step also relates directly to the intentions of the terrorist. The type of pathogen selected becomes essential to the type of possible attack. Using anthrax would allow for an attack against a specific target that could cause mass casualties over a defined geographic region. The area may be large and casualties high, depending on factors such as deployment method, virulence of the biological material, concentration to the weapon, weather conditions, and susceptibility of the population, but it would be contained within a predictable footprint. In fact, deployment in this manner would yield results more in keeping with what one would expect in a chemical attack. Casualties could measure in the hundreds of thousands or even millions, according to some studies, such as the 1993 OTA report cited above. However, anthrax would not be effective for a doomsday scenario. Such an attack would need to use a highly contagious pathogen such as smallpox. Even smallpox, unless genetically altered to make it impervious to the current vaccine, would not result in an "end of the world" scenario and likely would be controlled by using similar techniques as applied in the previous eradication campaign.

While not meaning to trivialize this first step, one begins from the premise that material suitable for developing a BW capability is naturally occurring and can be found in a variety of laboratories and storage facilities around the world, such as the ATCC in the United States. While many of the loopholes associated with unauthorized personnel gaining access to ATCC stocks have been closed in the United States, the same cannot be said for all nations or commercial entities that work with these pathogens. We also know from a recent GAO report that theft is another potential proliferation window. Additionally, some the BW material can be produced easily in a laboratory. *Clostridium botulinum*, the organism that causes botulism poisoning, can be created in a laboratory using commonly found material and limited technical knowledge, as discussed earlier in Chapter 2. The same is true for many other biological toxins that can be derived from naturally occurring and readily available biological sources.

We know that attempts by terrorists to acquire such exotic pathogens such as Ebola have failed in the past. However, the availability of these

pathogens around the globe can be seen daily in monitoring such websites as CIDRAP from the University of Minnesota, or the ProMED, a global electronic reporting system sponsored by the ISID. Both of these websites provide daily updates on infectious human and zoonotic diseases around the world.

At this point, a cautionary note is in order. The evidence certainly indicates a terrorist organization could gain access to pathogenic biological material. However, this does not imply a terrorist could gain access to all types of pathogenic material. Clearly, limitations would prevent access to certain pathogens. Smallpox has been eradicated as a naturally occurring pathogen, with the only known stocks held by the United States and Russia. Chasing diseases around the world, such as al-Qaeda attempted with Ebola, may make obtaining those diseases that occur episodically difficult as well. Obtaining the right type of a certain pathogen could also prove challenging. However, the evidence suggests that acquiring pathogenic source material for use in an attack is well within the reach of a determined terrorist organization. Consider that both the hantavirus and *Francisella tularensis* responsible for HPS and tularemia, respectively, are endemic to the United States and together cause several hundred casualties per year due to natural sources of infection. They are also considered potential BW agents.

The next two steps in the engineering process are closely related: processing and weaponizing the acquired seed material into refined pathogens with the characteristics desired for employment in an attack. The literature concerning developing these capabilities indicates increasing availability of the resources required for these steps, including the knowledge necessary to perform this preparation. In short, advances in biotechnology suggest these steps are becoming technically less challenging.

A basic kit for the processing of seed stock into the quantities required for taking to the next step of weaponizing of the bacteria or virus is not particularly sophisticated. Such a kit can be approximated using common equipment found at a home improvement store. The list of dual-use equipment for export control provides an initial shopping list for a terrorist program and includes fermenters (capacity equal to or greater than one hundred liters), centrifugal separators (capable of flow of one hundred liters per hour and steam sterilization), cross-flow filtration equipment (equal to greater than five meters), and freeze-drying equipment. In addition, some sort of PPE would be required, although it could likely be improvised and still be effective against most bacteria and viral agents, given careful handling.

This brings us face to face with the dual-use issue. While perhaps not seemingly related at first blush, similarities exist between the development of bioweapon material and such industrial processes as beer making. Both are biologic procedures in which a fermenter is used to drive a fermentation process in which microorganisms are grown. While home brewing kits would be highly inefficient, commercially available systems such as those used by microbreweries could easily serve the purpose of developing biological weapons.

Separating the agent from the byproducts could be easily accomplished using a standard centrifuge. While not particularly efficient for large-scale production, the use of a centrifuge or even several centrifuges would be adequate to produce a sufficient quantity for terror attacks with more limited aims. If even a fraction of the potential noted earlier in Chapter 2 from some of the assessments from the WHO, CRS, or the U.S. government's experiments (such as the anthrax-filled light bulb deployed in the subway that scientists estimated could have infected up to a million passengers) were to be achieved, a very small amount of material would have a significant effect.

Likewise, a simple drying system could be configured. The key to drying is establishing an area with low humidity and a source of medium heat so as not to harm the material while removing the moisture. Experts have also indicated the ease with which this part of the process can be managed using a lyopholizer or freeze-drying equipment, which would allow for quickly converting wet germ cultures into dried agent. However, more crude methods could also be used.

In laying out the case against Dr. Bruce Ivins, the now-deceased scientist accused of perpetrating the Amerithrax attacks in 2001, speculation is that he used these more rudimentary drying methods. An article concerning the investigation provides a cautionary note indicating the drying step could have been carried out with equipment no more complicated than a kitchen oven. Of this technique, Sergei Popov, a former Soviet bioweapons scientist who now specializes in biodefense at George Mason University, in Fairfax, Virginia, relates the relative ease with which the basic procedure could be accomplished. At the same time, he notes it would be difficult to reproduce the results. Popov also notes that going too fast in the drying process yields "sand," and therefore the potential bioterrorist would need to be cautious in this technique. In fact, he attributes the variance between the first and second batches from the Amerithrax attacks to this learning curve, noting that the product was greatly improved in the second batch.[4] All of this illustrates the propagation of information concerning the development

of these capabilities is proliferating in a dangerous manner, and that the capabilities required can be quite modest.

Turning the dried material into a fine power could also be accomplished using easily obtainable equipment. For example, one solution, although makeshift, could entail using a sealed canister such as a coffee can with marbles inside into which one could place the dried material. Then, either manually or mechanically, one could begin the milling process until the desired size agent is achieved. While the solution may lack elegance, it certainly could be effective in preparing the agent for dissemination.

Weaponizing a pathogen—going from the "raw material" to the product to be used in a weapon—is related to the type of delivery system to be used in the attack, the pathogen to be employed, and the desired effects to be achieved. Additionally, weaponizing the BW material introduces a degree of risk because it calls for increased handling and the accompanying potential for accidental release or exposure. However, given basic protections and the right motivation, the thresholds for weaponizing a BW pathogen are continuing to be lowered and will soon be well within the reach of today's terrorists.

Also important to the question of whether a terrorist could achieve a BW capability are the facility requirements. We have already alluded to these rather modest requirements, but they are worth reviewing. Several pieces of equipment have been identified as required or at least desirable for building a BW weapon. The term "desirable" was used to signify that field-expedient capabilities could be used in lieu of the actual piece of equipment, should it prove too difficult to obtain. However, even with the list provided, all necessary components could fit inside a ten-foot by ten-foot area, with limited facility requirements for power. The only specialized facility requirement would be the capability to ventilate the room to protect the workers. Additionally, the signature would be very small, almost negligible, throughout most of the process. The only significant signature would occur if there was a release during the process that was ventilated to the outside where it might be identified using a sensor, perhaps from the BioWatch program. Therefore, searching for an illicit BW lab is truly looking for the proverbial "needle in a haystack."

Regardless of the pathogen to be used, terrorists likely would want their bioweapon to be highly virulent, to remain so during dispersal, and to retain those properties in storage and during deployment. Techniques are available to increase the stability and encapsulate the material to make it more resistant to environmental degradation. As discussed throughout this volume, literature on these techniques is readily available. The advances in

biotechnology that included stability and encapsulation are continuing to advance at 400 percent per year.

Another important development in considering the ability of a terrorist to develop a BW capability is the increasing number of knowledgeable individuals with the skills either to engineer pathogens to increase virulence or to develop designer pathogens. As the field of biotechnology matures, more people are gaining access to the knowledge and capabilities necessary to make these genetic modifications. Events such as the following serve as cautionary anecdotes concerning this proliferation potential:

- Dr. Eckert Wimmer synthesizing a live poliovirus
- Dr. Mark Butler manipulating the mousepox virus based on a published article and inadvertently creating a more virulent strain of the virus
- Project *Bacchus*, sponsored by the U.S. government, developing a small lab for a modest investment
- an untrained individual experimenting with BW simulants in the "Kurtz case"
- the lack of restraint on the part of the scientific community with respect to the publication of potentially dangerous, dual-use information
- the general explosion of the biotechnology field

The next step in the process is planning the attack. The effectiveness of a BW event will ultimately be directly related to the planning. As in the case of the highly publicized use of a radiological "dirty bomb" that would use low-level radioactive material and conventional explosives, it is certainly possible to launch a BW attack using crude weapons and delivery methods. Historical examples include but are not limited to

1. the Mongols catapulting corpses contaminated with plague into Genoese fortifications, causing that population to flee (1346);
2. the British providing smallpox-infested blankets to the Indians in colonial America (1767);
3. the documented use by the Japanese of a variety of agents and employment methods against the Chinese in Manchuria (1932–45);
4. the Rajneeshee religious cult's crude introduction of salmonella bacteria into local restaurants in Oregon (1984);
5. the Aum Shinrikyo cult's attempted release on anthrax from the roofs of buildings in Tokyo (1994); and

6. members of a Minnesota militia known as the Patriots Council who intended to use ricin in an attack against law enforcement officers (1995).

While the "state-sponsored" BW attacks by the Mongols, British, and Japanese were somewhat effective, other terrorist organizations attempting to employ these weapons have not been particularly successful. This does not imply the threat of BW terrorism is not cause for concern, but rather that to date we have likely not seen the full potential of a bioterrorist BW attack based on a well-conceived and well-planned BW attack using appropriate biological material and dispersal equipment.

In considering potential bioterror scenarios, we must conclude the number and types of scenarios are virtually unlimited. The Los Alamos model, which considered more than 35 million scenarios for twenty-two different agents, provides some indication of the variety of possible attacks. Each pathogen has different characteristics that must be considered and that could result in different diseases. Biological agents can be spread by aerosol sprays, explosives, vectors such as mosquitos, contact through the contamination of food and water supplies, or even by using humans as BW weapons. Since BW weapons use living organisms, the attack profile has a significant impact on the overall effectiveness of the attack. Ultraviolet light, wind speed and direction, and atmospheric stability certainly affect outcomes. In fact, attack profiles vary greatly even within the same family of pathogen. Consider an attack using anthrax as the pathogen: three very different attacks are possible with three equally different outcomes.[5] By way of an example, we will consider the differences for three different types of anthrax exposures: inhalation, gastrointestinal, and cutaneous.

Inhalational anthrax requires the most refinement to ensure the particulates are of the appropriate size. If they are too small, they will be exhaled and not infect the host. If they are too large, they will not be suspended in an aerosol form and therefore will not be subject to inhalation. At the right size, one to five microns, the spores will both suspend in the air in an aerosol form and, once inhaled, remain in the lungs and eventually attach to the epithelial cells within the aveolis in the lungs. There the spores will germinate and the disease will begin to run its course. The course of the disease includes an incubation period of one to thirteen days, followed by twenty-four to forty-eight hours of fever, chills, cough, malaise, and chest tightness. A dose of ten thousand spores (but possibly as few as one hundred) may be sufficient to cause lethal infection. Left untreated, the disease will progress to respiratory distress, sepsis, and eventually death.

Another form of the disease is gastrointestinal anthrax. The incubation period is three to five days and the initial symptoms include twenty-four to forty-eight hours of fever, nausea, vomiting, and anorexia. The disease rapidly progresses to vomiting of blood, rectal bleeding, acute symptoms of the abdomen, and potentially severe pulmonary symptoms. Without prompt and proper treatment, death is inevitable. The size of the spores is less important for an attack by this route because even larger spores could be ingested and absorbed within the gastrointestinal tract.

The third form of the disease, cutaneous anthrax, has an incubation period of one to six days. It results in ulcerated skin where the contact occurred. The disease causes a blackened area of dead tissue of about two to three centimeters over a two- to five-day period. This variant of anthrax generally affects hands, forearms, head, and neck, but may also affect chest, eyes, and mouth. In about 20 percent of the cases, the patient succumbs to the disease. The spore size is much less important for cutaneous anthrax.

None of the three forms anthrax has documented human-to-human transfer. Additionally, the spores are highly sensitive to disinfectants—the recommended disinfectant is a 10 percent hypochlorite solution. In all forms, infection is based on contact with the pathogen, through either inhalation or contact. Treatment options, mainly consisting of antibiotics and supportive care, have a high degree of success if administered early in the course of the disease. Reports of resistant strains of anthrax have surfaced, but the use of broad-spectrum antibiotics would still likely have a positive effect.[6]

The point of this detailed anthrax discussion is to establish that the planning and scenario development for employment of the pathogen is critical. One can see that, given these very different forms of the disease, equally distinct forms of attacks (in terms of delivery method, desired effect, and potential for causing mortality and morbidity) would need to be contemplated. The use of larger spores for either cutaneous or gastrointestinal anthrax might be suitable for a small-point target. One could easily envision larger spores being used in an attack in a cafeteria in a government building or sent through the mail and distribution system in a manner similar to the 2001 Amerithrax attacks. Casualties would be expected to be fairly low and restricted to those having direct contact with the spores, but an attack in this manner would be possible.

If an inhalational attack were to be conducted, the refined spores could be deployed in the form of an aerosol blanketing an area. All initially exposed and potentially those involved in the clean-up, who might cause the spores to become airborne again in a secondary aerosol during the

decontamination process, would need to receive vaccine and antibiotic treatments. Given the wide area and the time elapsed between the launch of the attack and the beginning of treatment, casualties would vary greatly. The deadly potential of a highly refined inhalational form of anthrax can be seen in reports of the Sverdlovsk accidental release in 1979 that killed 66 of 96 people infected and continued causing symptoms over sixty days after the inadvertent release, and the Amerithrax attacks in which five of the eleven victims with the inhalational form of the disease died.

Unfortunately, given the complexity associated with the acquisition, development, weaponization, and planning of an attack, the deployment of the weapon to the point of attack and conducting an attack are not the most technically difficult steps within the engineering process described. Just as 9/11 reinforced, attacks can be launched creatively using capabilities solely intended for peaceful purposes—such as civilian airliners—and have devastating consequences. We should be prepared for this same creativity from bioterrorists in the execution of their attacks. The Amerithrax attacks in 2001 are yet another demonstration of how systems designed for peaceful purposes, such as the U.S. Postal Service, could be hijacked by terrorists for their attacks.

Given the relatively compact nature of BW weapons and the lack of telltale signs, such as in the case of nuclear weapons that would result in an explosion and a radiological signature, a BW attack would be very difficult to detect. In all likelihood, with some careful planning the terrorists would be able to deploy their biological weapon and be gone long before the effects of such an attack became evident. In fact, initial cases would probably not be detected as originating from a bioterrorist attack because people presenting at emergency rooms would likely have influenza-like symptoms and not begin to cause suspicion until the numbers grew to well beyond expected norms. A biological weapon deployed during the normal influenza season would probably take even longer to isolate to establish definitively an attack had occurred.

Throughout the discussion of the five steps for developing a terrorist BW capacity, an implicit assumption has been that knowledge would be necessary to achieve each of the steps individually and then to combine them collectively into an attack scenario. This is where globalization—advances in communication, transportation, and information technologies—has worked against our ability to keep these processes and capabilities out of the hands of those not requiring them for legitimate research and medical requirements.

The global proliferation of knowledge in all areas has greatly reduced the threshold for developing BW. The Internet is a virtual market where goods and services are bought and sold or even left "lying around" for anyone to find them. If you want to know how to process a particular pathogen, you will likely find helpful information on the Web. If you want the genomic sequence of a pathogen, another website is easily accessed that lists a wide variety of pathogens, including CDC-controlled Category A, B, and C material (see Appendix C). If you want to buy a fermenter or freeze-drying machine, you can order one from the comfort of your home. Even information available from sanctioned research is available on the Web. If you have an interest in anthrax weaponization and deployment, there are numerous journal articles that describe techniques that are useful in controlling pathogenity.

The articles concerning the Amerithrax attacks and the alleged perpetrator provide but one example of this tension between our desire to know what happened and our need to protect the methods used in developing the weaponized anthrax. An astute terrorist would certainly be able to learn quite a lot concerning anthrax development by examining the published material concerning the attack in the days and weeks following the suicide death of Dr. Ivins.

Given these concerns, it is prudent to secure information in the same ways we have chosen to secure the pathogens and biological precursor material. In fact, it is irresponsible to release controlled information that could potentially contribute to the development of bioweapons. Unfortunately, the proliferation of knowledge today continues with little more than the discretion of the scientific community as the final arbiter. We know, for example, that open source material was used to support the Iraqi biological weapons program, including information made available by the SIPRI.[7] Additionally, little government oversight exists with regard to education and basic research. It makes great sense to increase government visibility, encourage responsible behavior (such as ensuring trade journals control what they publish), and increase international cooperation.

As ever-increasing numbers of foreign students are educated in U.S. schools, "proliferation" will undoubtedly increase as well. Of course, this is a double-edged sword. On the one hand, there must be concern with the proliferation of these technologies. On the other hand, the potential for foreign students to learn Western standards of biosafety and biosecurity and then take these procedures back to their home countries assists in countering proliferation.

While this section has presented the five-step process for development of a bioterror capability, the next section will deal more directly with the technical capabilities required primarily in the processing, weaponization, and deployment steps articulated previously. As we will see in the next section, these technical capabilities are becoming less of an obstacle, given the meteoric advancements in biotechnology.

Trends in Biotechnology

Given the previous discussion concerning the steps necessary for developing a terrorist BW program, a reasonable question concerns how general trends in biotechnology will affect the ability of terrorists to develop a BW capability. "Militarily Critical Technologies List Part II: Weapons of Mass Destruction Technologies" from the DoD provides a useful point of departure.

Important trends and insights can also be gleaned by examining the health industry and public health in our society. In the United States today, the health-care industry comprises a $2.5 trillion industry out of a $13 trillion GDP. This reflects a market share of almost 20 percent of the total GDP, a staggering percentage. Any attempts to place limits on these types of activities likely would be cause for industry concern, and adversely impact potential advances that could benefit humankind.

Today, we are seeing advances in medicine resulting from R&D, refinement of medical procedures, and emerging technologies challenging traditional values, concepts, and beliefs. Legal systems and control measures have not kept up with theses advances, with the industry largely on autopilot. The work done as part of the manipulation of the genomes of living organisms is but one example of such groundbreaking work that has and will continue to alter our lives in dramatic ways. Ray Kurzweil's assertion that human life could be extended to 150 years and perhaps longer dramatically underscores these advances.

The military critical technologies graphic presented in Figure 2–1 depicts the relative change over time in several key technologies required for BW weapons development. The changes depicted were linear, showing how biotechnology fields have evolved in the period 1940–2000. Another way to examine the data is to analyze the percent change over time. In this way, one gets a better sense of the magnitude of the change the field is undergoing. The point is not just that capabilities in these technologies are doubling every six months, but that capabilities in these areas are increasing at an almost unfathomable rate.

Consider the field of the Human Genome Project, which is listed as doubling every six months since its inception in 1989. In the eleven-year period from 1989 to 2000, this area has seen an incredible growth of more than 4 million times more capability—of course, that is to be expected with a doubling in the field every six months or a 400 percent annual growth rate. With this sort of compounding, the increases in biotechnology will undoubtedly reach levels leading to extraordinary breakthroughs in the medical, scientific, and health fields, as well as to expose a critical BW proliferation window.

While the leading-edge science is continuing to see unprecedented growth, the "center of mass" of these fields is also changing dramatically. The example used in Chapter 2 was PCR, discovered in 1983. PCR is now a common analytical technique used for a variety of applications from sensors to DNA fingerprinting to gene therapy research. In other words, these technologies have gone from cutting edge to ordinary in a relatively short period. As these technologies become mainstream, access to them will increase. Just as we have observed with other technological advancements, the likelihood that they will be misused will also increase as terrorists may see them as a positive way to further their causes.

Imagine a terrorist with the scientific knowledge to engineer pathogens to make certain genes express themselves, thus increasing the virulence of a pathogen by an order of magnitude or being able to encapsulate the pathogen to make it more stable in the environment. Consider a scenario whereby a terrorist was able to manipulate the bacteria *Francisella tularensis*, which causes the disease tularemia. Perhaps as a result of the manipulation, instead of requiring ten to fifty organisms to cause infection, the dosage is reduced to require only one to five bacteria. Alternatively, perhaps the terrorist altered the virulence so the bacteria was antibiotic resistant and the mortality raised from 35 percent if left untreated to 95 percent if left untreated, or even to 35 percent if treated.[8] These would be frightening outcomes for society and the public health community.

An even more frightening development would be the synthesis of the smallpox virus, now eradicated, using these advanced biotechnology knowledge, techniques, and equipment. Some might argue this is a technological schism no terrorist group will be able to cross. As several key events demonstrate, however, this may not be a valid assertion. Dr. Eckert Wimmer demonstrated the technology for creating a live poliovirus using synthetic material. The poliovirus is a Class-4 RNA virus from the *Picoraviridae* family that typically has seven thousand to eight thousand base pairs as part of its genomic sequence. In contrast, smallpox is a Class-1

DNA virus from the *Poxviridae* family. It has approximately 200,000 base pairs and approximately two hundred genes.[9] In comparison to the poliovirus, smallpox has greater complexity in both size and structure. Still, the genomic sequences for both these viruses are readily available—on the Internet, in fact. So while there are differences between the two in scale and complexity, to be sure, with biotechnology maturing at 400 percent increase per year, it seems only a matter of time before we are able to synthesize smallpox using these same recombinant technologies. If we are able to do so, when will we reach this level of sophistication and be able to accomplish this feat—2010, 2020, 2030?

As we contemplate this question, we must consider that the proliferation of advanced equipment and techniques is rapidly lowering the threshold for gaining access to many of these technologies and capabilities. Recombinant technology to build biological capabilities is no longer the province only of those working at the cutting edge. Gene synthesizers are commonplace in labs, pharmaceutical companies, and even in many universities. This equipment can make genes for use as primers in PCR analysis that is important for testing and sensors. However, if one knows the genomic sequence—which, as stated before, is readily available—it is possible to synthesize biological material.

The Amerithrax attacks have also had an interesting yet ominous effect on the proliferation of these types of capabilities, as well as on the number of facilities available for handling the most highly pathogenic biological material. In fact, both are beginning to proliferate, in some cases leading to even a greater threat. Since these attacks, the number of BSL-3 and -4 laboratories—those able to work with CDC Category A and B agents—has dramatically expanded, which has led to a complementary proliferation of knowledge and capabilities, as well as to an increase in the storage of these dangerous pathogens in more areas around the country. In fact, as discussed earlier, we are not even clear about the actual numbers of these facilities.

This discussion is not intended to imply that BW will become as readily available and used as often as an AK-47 assault rifle or C-4 explosives, but rather that the thresholds for developing biological weapons have been considerably lowered through the biotechnology revolution. Given the continued expansion of the biotechnology field and the economic incentives to do so, it is highly likely these trends will continue and the technical thresholds will be lowered even further.

Even if the biotechnical capabilities necessary to develop BW remain too sophisticated for a terrorist to master, the proliferation of these

technologies leads one to possible scenarios whereby a terrorist organization could seek to obtain some of these pathogens through blackmail, theft, or even from a sympathizer with knowledge of biotechnology who might be willing to serve as a supplier. Building on one of these scenarios, if a knowledgeable terrorist trained in basic laboratory skills were able to obtain viable weapons-grade BW material, it is entirely possible to project he would be able to grow enough material for use in an attack or even alter a pathogen to make it antibiotic resistant, and then conduct a successful large-scale attack.

The Amerithrax attacks should serve as a final reminder that these advanced capabilities have allegedly already been used in a successful terrorist attack. While much of the information concerning the attack remains within law enforcement channels, by all accounts the material used had been successfully processed and weaponized. Of course, today we believe the material was produced in a U.S. facility and therefore developed using laboratory-quality facilities, highlighting this potential proliferation window from a legitimate source.

What History Has Taught Us

Fortunately, the history of terrorist use of biological weapons is limited. Therefore, few case studies are available from which to obtain useful information. Most of this history concerns hoaxes and pronouncements, with only a handful of actual programs or attacks to study and on which one can base conclusions. Another large percentage of previous BW programs include attempts to poison specific targeted individuals using such pathogens as ricin, and would be more in keeping with criminal activity than with a terror plot.

However, three cases in particular are worthy of examination in attempting to understand the potential for a bioterrorist attack in the future: the Rajneeshees, Aum Shinrikyo, and the Amerithrax attacks. A useful depiction of the significance of these three cases to the overall examination of the potential for a terrorist BW attack is provided in Figure 4–2. The figure also establishes the relationship between capabilities, intentions, and knowledge, and the potential for an attack in the future. It clearly depicts that increases in biotechnological capability and requisite knowledge coupled with the increased desire for more violent and spectacular terrorist attacks are leading to a complementary increase in the probability of a viable bioterrorist attack.

The x-axis depicts a sixty-year time horizon, with 2009 in the center. The y-axis depicts the probability of a terrorist conducting a viable attack.[10]

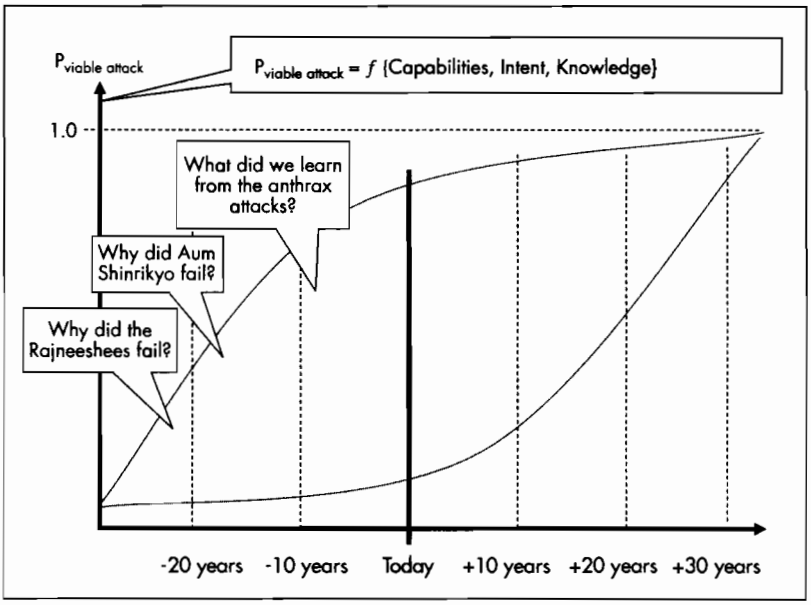


FIGURE 4–2 Examining the Potential for a Bioterrorist Attack

The boxes in the figure ask three basic questions about the attacks to be examined in this section. The elliptical polygon in the diagram depicts the probability of a terrorist conducting a viable attack in the future. The solution space, depicted by the polygon, shows that the probability of a viable attack is increasing and will likely approach 100 percent at some point in the future based on both the proliferation of biotechnology knowledge and capabilities and general globalization trends that provide a greater availability of means for perpetrating a BW attack for those terrorists with the intent to do so. Of course, without the intent to employ BW in an attack, the conditional probability of a viable attack is reduced to the lower part of the polygon.

By way of an example, in considering the potential for a BW attack in 2030—approximately twenty years in the future—the probability of a viable attack would vary from approximately 50 percent to 95 percent, based on the likely technical capabilities at the time and the desire of the terrorist to engage in this sort of attack. Just as with the other models considered, the variance can be explained by such factors as (1) technical prowess, including biotechnology capabilities, (2) the technology base of the location in which the development of the pathogen occurs, (3) the education level of the terrorists, and (4) the intentions and motivations of the terrorist including decision making: normative constraints, constituent

constraints, state sponsor constraints, religious constraints, and internal politics within the group. Over time, as the technical capabilities continue to proliferate, the viability of conducting an attack would be related more to the intentions and motivations of the terrorists. Thus, the overall probability increases toward 100 percent for those groups desiring to engage in this type of attack.

In looking at the Rajneeshee incident, some might take issue with the categorization of this effort as a failure. The author has chosen to do so because the scenario and attack were not sufficient to achieve the desired outcome (i.e., the changing of the electoral balance in a local election). This is true although, when the attack was conducted, the motives were more about being a nuisance or retaliating than for any greater purpose. Additionally, the final target selection indicates a "target of opportunity" rather than a carefully considered attack with realistic goals and objectives.

While the attack sickened more than 750 people, the crude methods of development of the material and the crude attack itself indicated a significant lack of technical capability. In fact, had the perpetrators been working with a highly pathogenic agent, they would likely have sickened themselves based on their sloppy lab techniques and failure to use PPE. Still, the attack demonstrated that a determined group could obtain source material from a legitimate source (although their loophole has now been closed), our food supply was extremely vulnerable, and epidemiological capabilities resident in the small city of The Dalles, Oregon, and more generally nationwide, were not sufficient to rapidly identify an ongoing BW attack.

Aum Shinrikyo presents an interesting dilemma. The group was extremely well funded and had biological and laboratory expertise within its ranks. They experimented with several pathogens including anthrax, botulinum toxin, Q-fever, and Ebola virus, but were unable to successfully develop BW weapons before deciding to conduct a chemical attack using sarin gas. That attack was successful.

In examining the Aum Shinrikyo case, one clear assessment is that the means available were completely inconsistent with their stated goals because their methods could not possibly have led to accomplishing the strategic outcomes they desired of ending the world. None of the pathogens in which they had previously expressed interest would have applicability for use in a catastrophic doomsday scenario. Their techniques demonstrated an inability to successfully use the five steps in the BW development process:

- They attempted to use variants of the pathogens that were not pathogenic to humans.
- Their attempt to release anthrax as documented in the picture of the plume of material emanating from the top of a Tokyo building indicates the processing of the material was inadequate and certainly not to the proper size for a successful inhalational anthrax attack.
- There is no evidence they attempted to manipulate the pathogens using advanced biotechnology to increase stability, virulence and ultimately their chance of success.

Furthermore, the crude deployment methods called into question their ability to understand how to deploy either CW or BW. In the case of the subway attack, they placed the liquid sarin in plastic bags. At the time of the attack, they poked holes in the bags, resulting in a release of the agent. In the case of the oft-ridiculed anthrax operation, one can see in the picture of the attack a thick plume emanating from an aerosol device on the top of a Japanese building using particles far too large to be used in such an attack. Furthermore, they used a form of anthrax that was not pathogenic to humans.

The Amerithrax attacks in 2001 provide ample evidence of the potential for a terrorist BW attack using a mix of capabilities. The pathogen appears to have been well prepared to the appropriate specifications in terms of size and pathogenity. First-hand accounts discuss the material floating in the air and the ease of re-aerosolization just by moving close to the material as it was sitting on a countertop. The deployment methods, however, were simplistic. Placing the anthrax in envelopes and mailing the material along with threatening letters was relatively unsophisticated. Still, on balance, the attacks were successful, although even now the motivation remains a mystery. The most important aspect of the Amerithrax attacks was the reminder of a significant proliferation window with the potential for theft from a legitimate source that would go undetected until after an attack and require significant forensics work to trace the material back to the source.

Two other incidents are also worthy of consideration for considering the potential for developing BW capabilities. The U.S. government's investigation into the potential for developing a BW weapon as part of Project *Bacchus* certainly demonstrated that the development of these capabilities is not particularly complex or costly. In this case, the DTRA sponsored a study to determine if a group of scientists could develop an "anthrax" weapon. The group used a simulant, *Bacillas globigii*, for their work to avoid violating the BWC, but concluded that it was indeed possible to

develop such a capability using modest means, equipment, and facilities. The second incident is the Kurtz case mentioned above, in which a nontechnical individual was able to acquire and weaponize a BW simulant for use as part of his performance art. This incident provides valuable insights into the degree to which a nontechnical individual with open-source material can develop significant bioweapon techniques and capabilities.

Two notes of caution are in order. First, while capabilities will continue to proliferate and the potential for large-scale attack will continue to increase, biological weapons are living organisms and will continue to be sensitive to their environments. They can easily be destroyed if not handled appropriately. Given these limitations, some pathogens may prove elusive for incorporation in a terrorist's BW repertoire. Second, just as when one goes fishing, the type of fish caught depends on where one casts the line. So, too, with biological weapons: not all pathogens will be available for a terrorist to use in a BW weapon. Therefore, a secondary conclusion is that some pathogens will likely be too technically challenging to employ or else will not be physically available.

Overall, however, we must assess that thresholds for acquiring a BW capability and conducting a successful attack have been significantly lowered through a combination of the proliferation of the scientific knowledge, increasing biotechnical capabilities, and the growing trends in globalization placing more powerful capabilities in the hands of potential terrorists. The dual-use nature of BW makes this finding even more certain. Simply stated, the evidence strongly suggests it is possible now and will be more possible in the future for terrorists to develop and deploy BW capabilities. The issue with regard to the potential for a bioterror event in the future will come down to the question of motivation and intent.

Understanding Terrorist Intent with Regard to Biological Weapons

Understanding terrorist capabilities and intent are crucial when assessing the likelihood of an attack. As many of the models considered previously indicate, examining technical capabilities is clearly less complex than assessing intent. Furthermore, given the increasing availability of BW capabilities and the conclusions presented above, it becomes all the more critical to understand the intentions of the terrorist. Judging their intent will always be difficult, however. One must understand the motivations of the terrorist to assess the conditions under which certain actions or weapons might be used. This is especially true with regard to WMDs, where international norms strongly argue against their use under

any conditions. In cases where state actors have employed WMDs, the international outcry has been significant. For example, Saddam Hussein gassing the Kurds certainly contributed to the 2003 United States–led invasion to oust him from power.

In understanding the potential for terrorist use of BW, several emerging trends are useful as harbingers of what the future might hold. First, the data suggest thresholds associated with level of violence as measured in terrorism fatalities have been altered with the U.S. embassy bombings in Tanzania and Kenya in 1998. Before those events, the number of fatalities was approximately 250 per year, on average. The Africa bombings, 9/11 attacks in the United States, and bombings in London, Madrid, and Bali indicate a trend toward larger, more deadly events against purely civilian targets.

Second, continuing globalization has created the perfect environment for fomenting discontent and airing grievances on the world stage. The twenty-four–hour news cycle and nature of reporting provides both a cause for and a means of getting one's message out. If one wants to get on the evening news, a suicide bomb that kills three people including the bomber will likely get only a mention, if that. However, a bombing that kills hundreds, such as the bombing of embassies in Africa, will make news for weeks, months, or even years to come.

Third, the databases and literature all indicate that several major terrorist groups and some loner actors have expressed an interest in biological weapons. A number of hoaxes also signify terrorist interest in biological weapons, if only for the purpose of inciting fear. Clearly, al-Qaeda has signaled an interest in at least examining these weapons, although it is unclear from the literature whether they want to use them or simply talk about their use by way of a threat in order to gain notoriety. For instance, as recent evidence from actions in Iraq by AQI demonstrate that when violence was excessive or directed toward the civilian population, the support of the populace diminished. The nature of BW suggests that, in almost any scenario, civilian casualties would be very likely.

Fourth, in considering the potential for terrorists developing BW capabilities, we must consider the full range of motivations that could cause them to seek to acquire these systems. Some terrorists may want to develop these capabilities for use in an attack. Others may simply want them for status or to use as a deterrent. The degree to which terrorists find BW interesting will be related to their motivations. Terrorists groups such as the Irish Republican Army (IRA) that are moving toward becoming political entities are unlikely to be interested in developing BW capabilities. They would likely see developing these capabilities as

contrary to gaining acceptance and promoting their cause. Groups such as al-Qaeda, which are actively fighting and who rely on the support of the populace for financial and ideological support, may also approach large-scale use of BW with caution. This caution may come in the form of carefully selecting those targets to attack with BW to ensure they are "military" objectives or perhaps only threatening BW use versus actually conducting an attack. Apocalyptical groups such as Aum Shinrikyo will likely be more inclined to employ BW capabilities in large-scale attacks. Another subset of terrorists that has used BW in the past is the lone actor using a substance such as ricin to target specific individuals. We should expect this use to continue.

Fifth, strong international norms that argue against use of these weapons will prove to be a moderating factor for some. However, many terrorist organizations, especially those involved in active fighting, will believe, as bin Laden says, "acquiring weapons for the defense of Muslims [is] a religious duty. . . . It would be a sin for Muslims not to try and possess the [unconventional] weapons that would prevent the infidels from inflicting harm on Muslims."[11] However, we must also exercise some caution in looking at the statements such as those of bin Laden and understand that some of this rhetoric is likely for internal consumption and may not be a statement of intended policy.

Sixth, the technology associated with developing a BW capability will likely limit development of these capabilities to global terrorist networks or those within more-modern nations. A national terrorist group in an underdeveloped nation is far less likely to pursue these capabilities. If it does, it will need to rely on external support such as state sponsorship or theft to obtain them. The technological hurdles and danger posed by working with many of these pathogens, particularly those that are contagious or for which there are no treatments or vaccines, will effectively limit the population of agents terrorists will pursue, at least in the near term.

Despite the norms against such activity, the evidence suggests BW remains an interesting capability for the terrorists to investigate, develop, and perhaps even use. However, the decision to use BW will be based on individual preferences rather than on a generalization that would be uniformly adopted by all groups. The motivations and the sense of needing to mount increasingly more violent and extreme attacks will likely drive some terrorists toward developing a BW capability in the future.

Considered in its entirety, the issue comes down to this: Only a small subset of terrorist organizations will be able to muster the resources, capabilities, intentions, and support structure to engage in BW proliferation

in the near future. Even fewer would be able to mount a large-scale bioterror attack.[12] This is not to imply that the threat of bioterror is not credible or we should not prepare for it, but rather that we should understand the complexities associated with this threat make it a relatively low-probability yet high-consequence event.

The Adequacy of Current Nonproliferation and Counterproliferation Regimes with Regard to Terrorist BW

Nonproliferation and counterproliferation are two closely related activities designed to prevent the use and proliferation of dangerous WMD capabilities and technologies. Nonproliferation activities include dissuading or impeding access to or distribution of sensitive technologies, material, and expertise through diplomacy, arms control, multilateral agreements, threat reduction assistance, and export controls activities. Counterproliferation includes detection and monitoring, offensive operations, active defense, and passive defense taken to defeat the threat or use of WMDs. The two activities are designed to be used together, individually, and even sequentially, depending on the nature of the threat.

A cornerstone of the U.S. nonproliferation strategy includes the BWC. Unfortunately, the inadequacy of the BWC has long been recognized and contributes to a significant gap in our BW nonproliferation architecture. Several important issues combine to render the BWC largely ineffective for both state and nonstate actors. The lack of a verification regime in the BWC was in a sense the original sin. With no way to determine through an official verification regime if states were violating the provisions of the treaty, enforcement was virtually impossible. This shortfall has been well documented, and attempts have been made to strengthen the treaty provisions in this area. Despite these attempts, the treaty remains without any viable verification mechanisms.

If the lack of a verification regime was not enough to render the BWC ineffective, the fact the BWC is a treaty signed and enforced by nation-states at a time when the threat from state BW is decreasing while the terrorist BW threat is increasing provides further evidence the BWC in its current form is both ineffective and obsolete. The dual-use nature of BW weapons and the proliferation of biotechnology capabilities have more recently left the BWC all but irrelevant for anything other than an official declaration by a state as to whether it is a signatory and whether it is in compliance. Dual-use issues have seriously complicated any attempts to strengthen the BWC for state programs. This was illustrated at a 1997 United Nations

Educational, Scientific and Cultural Organization (UNESCO)–hosted conference on the "Possible Consequences of the Misuse of Biological Sciences." The conference's conclusions included the following:

> Dual-use technologies, materials and equipment have spread throughout the globe as biotechnology and pharmaceutical industries have grown. The widespread presence of dual-use technologies, equipment and materials in countries around the globe makes monitoring of the biological weapon proliferation very difficult. Tell-tale signs of a covert biological weapons programme are scarce and even discrete signs of a covert weapons programme can be hidden if a government is willing to pursue germ warfare in antiquated facilities without modern safety precautions, such as specialized containment facilities and worker vaccination.[13]

Furthermore, as we have seen with the U.S. Project *Bacchus*, even compliance is a matter of interpretation and is not necessarily an enforceable standard. However, evidence suggests fewer states are attempting to acquire BW capabilities. The international norms against use of BW capabilities, especially given the ever-increasing conventional capabilities available, remain extremely high and even may render these weapons obsolete, from a state's perspective.

Perhaps this dire assessment of our nonproliferation and counterproliferation capabilities as they pertain to BW is an overstatement? Surely, the means to process biological material into highly pathogenic substances must involve specialized equipment, carefully designed facilities, and highly controlled growing conditions? Unfortunately, this is not the case. We must also ask how far commercial dual-use capabilities have proliferated since 1997. The activities by groups such as the AG and the PSI have certainly been useful in raising the visibility of the issue. However, they are facing an uphill battle in attempting to stem the flow of dual-use equipment, technologies, and knowledge.

Because experts assess the inadequacy of the BWC for state programs and the lesser requirements associated with a terrorist BW program, it stands to reason the BWC will be even less effective in dealing with nonstate BW proliferation issues. In fact, Project *Bacchus* highlights the difficulties associated with attempting to detect small BW weapons programs. While a state program would have a modest signature assuming capabilities for storage and loading of the munitions were part of the program, the footprint for a small program such as one for a terrorist actor could be as small as a ten-foot-by-ten-foot room stocked with a modest amount of

readily available equipment. As the Kurtz case demonstrates, viable BW programs can be established in innocuous and modest surroundings, even in one's house. Because of the lack of a signature and the small facility requirement for a BW program, the counterproliferation issue becomes quite a challenge, at least for conducting offensive operations to eliminate terrorist BW capabilities.

Overlaying the N/CP activities with the doctrine for homeland security of "prevent, protect, respond, and recover," we see these activities pertain only to the "prevent" and "protect" areas of the doctrine. Prevention and protection are activities to anticipate, preempt, detect, and deter threats. Response and recovery are coordinated, comprehensive federal responses and the mounting of a swift and effective recovery effort.

To get a sense of overall preparedness and the difficulties associated with attempting to deal with the emerging terrorist BW threat, one can look systematically at the ability to interact across all five of the proliferation steps within each of the homeland security doctrinal areas. A graphical depiction of this analysis is provided in Figure 4–3. The matrix within the figure has been coded to reflect the ability we have to impact outcomes corresponding to "virtually no ability to affect," "some," and "significant," and "not applicable," respectively.

Given the nonproliferation issues discussed above, we assess "virtually no ability to affect" the *acquisition*, *processing*, and *weaponization* of BW material into weapons-grade material suitable for use in an attack for the *prevent* category, although we do assess

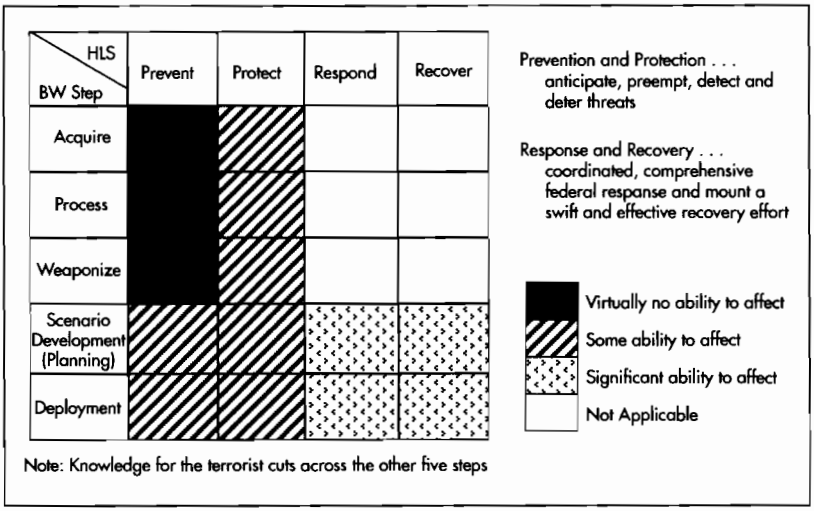


FIGURE 4–3 Two-Sided Analysis for Examining the Ability to Limit Terrorist BW

"some ability to affect" in the *protect* category. This rationale is based on the minimal requirements for BW development and the availability of naturally occurring pathogens. Concerning the *protect* category, some actions such as vaccinating populations against a certain pathogen can make use of this agent unattractive and therefore provide a degree of preventive measure. While these conclusions are supported by the evidence, they may not be universally accepted by some who still believe these BW development steps are considerably more technically challenging. However, given the increased knowledge available and proliferation of equipment, developing BW capabilities will prove to be less challenging in the future. This does not mean, as we discussed previously, all pathogens will be available: some may prove too difficult to handle or obtain, even once recombinant technologies become more readily available. This assessment is not to imply nonproliferation efforts should be totally abandoned, but rather that the thresholds for terrorists to obtain BW have been lowered; a fact we must recognize.

Examining the ability to *prevent* and *protect* terrorists from *planning* and *deploying* BW weapons, we clearly have "some ability to affect" moving toward "significant ability to affect" in the *protect* category. Effective measures will include (1) anticipating where the threats are likely to be greatest and taking countermeasures, (2) determining which pathogens are most likely to be employed and employing preventive measures, (3) deterring the threat through a variety of active and passive measures, (4) preempting the threat prior to deployment of a BW weapon, and (5) detecting the release of BW to allow for rapid identification of pathogens and clearing of the area under attack and treatment of victims. Certainly other actions could also be used. This list is representative, not all encompassing.

Other specific measures in the *protect* column of the figure for *planning* and *deployment* include increased use of sensors, red teaming to assess the likelihood of potential scenarios, and employment of passive defense counterproliferation measures.[14] Additionally, some nonproliferation activities will contribute to a more robust posture and therefore decrease the likelihood of a successful attack. We are continuing to see advanced biotechnology employed to improve sensor performance, improve protection from various pathogens that have the greatest likelihood of use, and increase awareness by governments and the public with respect to these issues. Success in the area of *protection* will be based on being able to provide more protective measures for which we have a greater degree of control, including:

- outside sensors for covering targets considered to be high value,
- greater stand-off distances between potential targets and access approaches,
- improved air-handling capabilities in buildings,
- inside sensors that detect anomalies in air quality and allow for rapidly activated low-regret options to be implemented, and
- enhanced vigilance by workers such as security personnel.

Coming to the last two columns of the figure, one sees two trends. The top of the chart is coded to indicate *respond* and *recover* have no relationship to the terrorist's ability to *acquire*, *process*, and *weaponize* BW material. The bottom two rows, corresponding to *scenario development* (planning) and *deployment*, are where we have the most opportunity to impact outcomes. As an example, sensors can be developed that facilitate both warning and treatment in real time. Better biosurveillance techniques and methodologies can be designed to reduce the time to detect outbreaks and attacks and establish the means and methods to prevent further infections. Many of these capabilities were discussed in detail in Chapter 3. Additionally, planning and exercises can be conducted to ensure that first responders, medical professionals, and public health specialists, as well as citizens, are able to respond effectively in a BW event.

Unfortunately, in most scenarios, the attacker has the initiative in determining the time and place of attack, complicating the ability of the defender to *prevent* and *protect*. An old military adage states, "He who protects everything, protects nothing." This sentiment remains operative for BW. It is both cost prohibitive and infeasible to attempt to *protect* and *prevent* against all types of attacks, or against the use of all types of pathogens in all types of scenarios. The result would be to turn the United States into a "BSL-4" nation, an infeasible outcome for a country that values civil liberties and basic human freedoms. Rather, guided by prudent assessments and based on the available resources, decisions must be made on what to protect and the level of acceptable risk.

We know from previous analysis that under the current nonproliferation and counterproliferation regimes containment of BW capabilities alone will not be a successful strategy. Certainly, measures can be put in place to mitigate against terrorist plots, but they are the least useful in the *prevent* category, more useful in the *protect* category, and the most useful in the *respond* and *recovery* categories.

We must further realize it is not feasible to attempt to put the biological genie back in the bottle. Biological advancements have already progressed

too far. Their ability to benefit humankind is too great to retrench in this field. Rather, society must come to terms with the understanding that fundamental building blocks of our educational, public health, medical research, and veterinary systems have the potential to allow for the development of devastating biological weapons.

The previous statements of the potential for a bioterror attack were prepared considering our capabilities in the near future, say in 2010, and were made without the benefit of classified material. Additionally, should a radical technological change to the environment occur or additional information become available, these assessments are likely to change. For example, as designer pathogens that may be invisible to certain families of sensors proliferate, we can expect even greater difficulty in preventing and protecting against a bioattack. Likewise, if this methodology were used for analysis in the year 2030, a different assessment is likely to result. Certainly, if we have been spending our resources wisely and the technology allows for more-sensitive and more-timely sensors to be deployed, we would expect a "significant ability to affect" in more areas over time.

Finally, this structured approach in considering the BW question results in a more refined assessment of the threats we face and the potential for affecting outcomes in this critical area. Therefore, the author believes that assessments employing this methodology should be conducted periodically to understand the shift that is occuring.

Identifying Essential Capabilities

The basic premise of U.S. policy has been that America requires a set of capabilities for preventing, protecting, responding to, and recovering from a BW event, should it occur. Singly focusing efforts for keeping BW capabilities from entering the country or out of the hands of a terrorist will not serve to protect the American people. Likewise, having no sensor or monitoring capabilities and allowing a potential attack to come as a complete surprise until the first symptoms appear puts us in the position of playing defense in a one-sided game. Similarly, building a "BSL-4 nation" undermines the foundations on which our nation was founded and would go far beyond the threat before us.

Instead, we must have strategies that can negate the effects of a likely attack and make use of these types of systems less attractive to terrorists. In framing the issue, some experts argue that the focus on BW, especially in the aftermath of the Amerithrax attacks, has detracted from other more pressing medical needs such as research in cancer and HIV/AIDS. Conversely, the hue and cry associated with the 2001 Amerithrax attack,

despite how relatively small and inconsequential the attack was in real terms, indicates the degree to which the issue is emotionally charged. Several questions define the subject for experts and policy makers. How much preparation is enough? What level of risk are we willing to assume? How much are we willing to sacrifice in terms of personal freedoms and liberties? And what can we afford?

For this analysis, we will focus on understanding the competitive aspect of BW looking at trade-offs between terrorists' capabilities and intent, and our level of effort to counter BW threats and attacks. Level of effort will serve as a metric for conducting this analysis, and level of funding will be the key index. The assumption will be that level of funding equates to effective and balanced expenditures commensurate with the spending levels.

In a unique approach, a game theory construct was used to examine this issue. These techniques seem ideally suited for use in this two-sided analysis of terrorists' potential for BW and our potential actions to counter these threats. They will allow us to delve into the motivating factors and moderating behaviors that drive the terrorists, as well as the actions and counteractions that the United States could take in addressing this complex issue. Game theory, simply put, is a distinct and interdisciplinary approach to the study of human behavior with mathematics, economics, and the other social and behavioral sciences being the disciplines most normally associated with this type of analysis. One source notes, "[Game theory] addresses the serious interactions using the metaphor of a game: in these serious interactions, as in games, the individual's choice is essentially a choice of a strategy, and the outcome of the interaction depends on the strategies chosen by each of the participants."[15]

For our purposes, game theory allows for a rational expression of outcomes based on the motivations of the actors involved. The capabilities and intentions of the potential bioterrorist can be pitted against the actions and counteractions we might take to arrive at a set of consequences. These results are depicted in a payoff table (or matrix) normally expressed as numerical values, where each cell in the matrix has two values, one corresponding to each of the actors involved in the game. In this analysis, given the uncertainty of outcomes and attempting to consider conclusions that are more strategic, the payoffs will be expressed as favorable, neutral, or negative outcomes.[16]

In our game, we will look at four possible terrorist actions: (1) divest of BW capabilities, (2) demonstrate interest only, but do not conduct a BW attack, (3) conduct a small-scale BW attack, and (4) conduct a large-

scale BW attack. U.S. efforts in this game in countering BW will include (1) a minimal level of effort, (2) a low level of effort, (3) a medium level of effort, or (4) a high level of effort. The levels of effort for the United States have been tied to the resourcing of biodefense and are further compared to the spending of more than $8 billion as of 2008.[17] Detailed explanations for each of the categories are provided in Table 4–1. Using this approach, we will attempt to understand the motivations of the actors involved and apply a level of rationality to the actions each might decide to take. For example, the intersection of the terrorist *divesting of BW capabilities* and the United States making *minimal effort to counter BW* forms a set of payoffs, one for each of the actors. Doing this across all four of the terrorist and U.S. potential actions forms a matrix with sixteen sets of possible outcomes.

The stratagem can be explained as follows: A terrorist would decide on a strategy to pursue by considering assessments, including capabilities and intentions. A certain payoff value would be possible, based on both his strategy and the strategy of the opposition (in this case, the United States). Likewise, the United States would decide to pursue a strategy. The value of that selection would be linked to the strategy pursued by the bioterrorist. The goal for each actor is to identify a strategy that provides the greatest potential for achieving his goals and objectives.

The strength of this analysis is to allow us to look not only at the capabilities and intentions of the terrorists, but also at the actions we can take to counter a terrorist BW threat. Previously, we discussed the five steps of the terrorists BW model and the potential for us to counter these activities through the homeland security doctrine of prevent, protect, respond, and recover. Our game theory approach builds on this previous analysis as well as on the earlier efforts to understand how capabilities and intentions have been factors within a historical context.

To provide more granularity to the analysis, we will examine three different categories of terrorists: traditional, waning, and apocalyptic (Table 4–2). The *traditional terrorist* relies on a range of activities from political to violence in pursuit of his objectives, yet is sensitive to retaining the support of its constituents. In this formulation, an action by the traditional terrorist results in a counteraction by the United States, and vice versa. The trade-offs continue as a series of actions and counteractions. An example is AQI following the U.S.-led invasion in Iraq in 2003. AQI attacked coalition forces, waged an insurgency, and attacked innocent people through bombings, attacks, and kidnappings. When the level of violence became too high for the populace to accept, AQI lost support and

TABLE 4–1 Explanation of the Game Theory Strategies

ACTOR	CATEGORY	DEFINITION
Terrorist	Divest of BW capabilities	Includes (1) divesting of all BW capabilities and intentions for those terrorists that have been involved in these types of activities, or (2) continuing to not demonstrate interest for those terrorists that have no active program or have never sought to acquire these capabilities.
	Demonstrate interest only, but do not conduct a BW attack	Includes all forms of BW in the steps necessary to acquire BW up to the deployment phase of the model. It can include planning, however no active measures for perpetrating an attack such as target reconnaissance would be conducted.
	Conduct a small-scale BW attack	An attack against an area target with BW capabilities that causes mortality and morbidity of less than one thousand. Normally, such an attack would employ noncontagious pathogens using such agents as anthrax or tularemia.
	Conduct a large-scale BW attack	A BW attack that causes mortality and morbidity in excess of one thousand people. Attack could be perpetrated using contagious or noncontagious pathogens.
United States	Minimal effort toward countering BW	Would see a return to pre-Amerithrax attack BW spending levels of less than $500 million per year. Would leave the United States with the current capabilities frozen as they are today with no modernization plans. This level of funding would essentially leave us unprepared for either a small- or large-scale attack.
	Low level of effort	Reduction of current counter-BW spending to less than $4 billion per year. This represents a 50 percent reduction over 2008 spending. Would freeze the current BioWatch, BioSense, and BioShield programs at existing levels with no further enhancements. Would essentially leave the United States unable effectively to a large-scale attack and put at risk preparedness and response for a small-scale attack.
	Medium level of effort	Increase 2008 levels of BW funding slightly to more than $10 billion per year. Continue modernization of the BioWatch, BioSense, and BioShield programs. Continue to raise visibility of counter-BW efforts. Would improve biosurveillance and response efforts, allowing for a coherent response to a small-scale attack, but with limited capacity for large-scale attack protection or response.
	High level of effort	Double BW spending to $16 billion per year. Aggressively field new generation BioWatch, BioSense, and BioShield capabilities. Raise the level of visibility for BW to make it a key policy issue for natianal security. Would provide capabilities for successfully managing a small-scale attack and would better prepare for a large-scale attack.

adjusted its tactics to reduce civilian casualties. An overwhelming majority of terrorist groups fall into this category of traditional terrorist.

TABLE 4–2 Terrorist Categories

Category	Description	Example
Traditional	• Conduct a range of activities from political activities to violence • Support of populace and constituents key • Represents the majority of terrorists	al-Qaeda
Waning	• Looking to achieve their objectives through political, social, and economic means • Use of violence contrary to their objectives • Support of populace and constituents paramount	IRA
Apocalyptic	• Very small number of these types • High violence as part of their strategy • No negotiation possible	Aum Shinrikyo

The *waning terrorist* began by using a range of activities from political to violence in pursuit of objectives, but over time has begun to move toward becoming a political organization and therefore tending away from violence. Terrorist organizations in this group are therefore less likely to become involved in BW because doing so would detract from the progress they have made in becoming political entities. The waning terrorist also is keenly focused on maintaining support from their constituents. An example of a waning terrorist group is the IRA.

Finally, *apocalyptic terrorists* include terrorists that have an ideology and intentions that will make involving them in any sort of action-counteraction game a near impossibility. The term "apocalyptic" is not necessarily intended to identify these terrorists as moving toward the apocalypse in a literal sense, but rather to indicate they have high violence strategies they will undertake, regardless of the actions of their adversary. Apocalyptic groups are insular and internally focused, using any and all available means to achieve their desired outcomes. An example would be Aum Shinrikyo, which would not have been dissuaded by any actions taken by the Japanese government or lack of support from the populace for their cause. Importantly, there are very few groups within this categorization of apocalyptic terrorists.

The first analysis will examine the outcomes for the traditional actor terrorist. As we have stated, this terrorist will be influenced by a number of different factors, making the outcomes across the solution space highly variable and subject to an action-counteraction solution. Several impor-

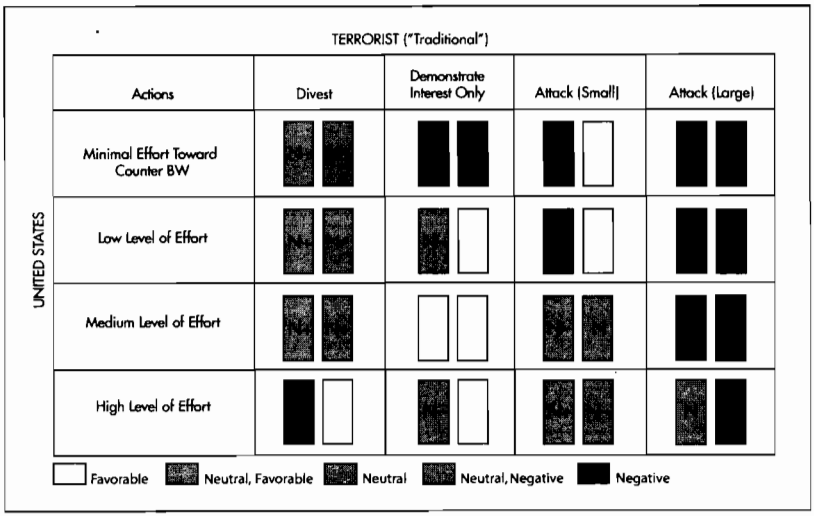


FIGURE 4–4 Game Theory Payoff Matrix for the Traditional Terrorist

tant assumptions serve to guide this analysis. First, the traditional terrorist wants to gain notoriety its cause. That need for notoriety becomes a driving factor in the actions it undertakes. Violence and the means used serve as tools, but they are not the ends of the strategy. Gaining and maintaining support from the traditional actor's constituency is important, and therefore plays a key role in the manner in which the terrorist acts, becoming both a motivating factor and moderating influence for the terrorist. The results are provided in the payoff matrix in Figure 4–4.

For the traditional terrorist, divesting of all BW capabilities and intentions would make him less of a perceived threat and therefore would likely lead to no increase in visibility for his cause. Therefore, the outcome for the traditional terrorist would be "neutral negative" for where the United States had minimal or low level of effort. The terrorist payoff of "neutral favorable" for the U.S. medium level of effort reflects that, despite divesting of capabilities and intentions in BW, the United States makes a significant commitment in terms of policy, programs, and spending. As the U.S. level of effort goes to high, which would represent a doubling of the current effort, the terrorist payoff changes to "favorable," reflecting that, despite the terrorist's divestiture in BW capabilities, the United States had "wasted resources" by overspending against a nonexistent threat.

Examining the payoff from the U.S. perspective for the terrorist divesting of BW, we see an interesting relationship. If the United States puts minimal effort toward countering BW and the terrorist divests of BW

capabilities, and intentions, the result is "neutral negative" for the United States. This assessment is based on the perception that, at these levels, the government would fail to demonstrate the capability to mount an effective biodefense posture, which would be seen as imprudent.

As the level of effort goes up to low, the U.S. outcome moves to "neutral favorable," indicating the measures taken and the level of support would be seen as prudent. The same rating would be gained from the medium level of effort. In both these cases the rationale would be that an appropriate level of effort commensurate with the threat would have been undertaken. As the level of effort goes to high, the assessment changes to "negative" because the United States' expenditure can be thought of as being wasted if the traditional terrorist has divested of his BW capabilities.

In the second case where the traditional terrorist demonstrates interest only, one sees a different payoff structure for both sides. For the terrorist, demonstrating interest includes actions such as public pronouncements, attempts to develop BW capabilities and perhaps even having a BW capability, but stops short of using these capabilities in an attack. In all cases, the increased exposure translates to "favorable" outcomes for the terrorist for each of the strategies undertaken by the United States.

From the U.S. perspective, in the case where the terrorist demonstrates interest in BW and the United States puts forth minimal effort, the government will be seen as weak and even imprudent for failing to take actions to anticipate, deter, dissuade, detect, and perhaps preempt the terrorist. Until the level of spending and capabilities is seen to reflect reasonable and prudent expenditures, the outcome will be "negative" or "neutral negative" at the minimal and low levels of spending, respectively, from the U.S. perspective.

The case where the terrorist demonstrates interest and the United States puts forth a medium level of effort reflects a "favorable" outcome for both. The terrorist gains notoriety for his cause, which results in an expenditure of resources. The U.S. government is seen as taking prudent measures to protect the population against a possible BW attack. As the level of effort rises, overexpending resources can begin to change the outcome from the U.S. perspective from "favorable" at the medium level to "neutral negative" at the high level of effort, because the effort is once again disproportionate to the threat.

In the third case where the terrorist perpetrates a small-scale attack, the payoff structure changes yet again. Several notes are in order at this point. The payoff structure will likely be highly influenced by the targets selected. If a "military" target were selected, the traditional terrorist's supporters

would likely not take great issue and may even express support. However, if an elementary or high school were attacked with a BW weapon, the traditional terrorist would likely lose support and even gain condemnation for the attack and perhaps even for his overarching cause. Despite the targeting question raised above, we assess the small-scale attack scenario as being "favorable" for the terrorist if the United States were to put forth minimal effort or a low level of effort. As the U.S. effort increases to medium, the terrorist payoff becomes "neutral." The attack would be less successful and mounting such an attack would introduce a degree of risk for the terrorist. At the U.S. high level of effort, a small-scale terrorist attack would be assumed to not be successful. Therefore, the assessment would be downgraded to "neutral negative" from the terrorist's perspective.

An important caveat: these ratings for a small-scale attack assume the attack was both against a perceived "just" target and the lack U.S. of preparation contributed to considerable casualties, but still below the one thousand threshold. Of course, the international norms against the use of WMDs, in particular BW, introduces a degree of risk because one could easily argue any use of BW would be considered irresponsible by the terrorist's supporters and therefore not worth the risk. Furthermore use of BW would likely result in a greatly increased level of effort against the terrorist. Certainly, in an age where there are other conventional capabilities that could be used to achieve desired outcomes commensurate with a small-scale bioattack, resorting to BW would seem to be crossing an important and risky threshold. This would be even truer should the agent be a highly contagious pathogen with the potential to threaten populations indiscriminatingly.

In looking at the payoffs from the small-scale attack scenario from the U.S. perspective, if the United States were to make minimal effort or only a low level of effort and an attack were launched, both strategies would be perceived as "negative" outcomes. In each, the result likely would be measured in increased casualties and a failure by the government to take prudent measures to protect citizens, property, and interests. If the U.S. government puts forth a medium level of effort and there is a small-scale attack, the outcomes are likely to be perceived as "negative neutral," assuming the preparations were reasonably effective and only moderate numbers of casualties resulted. The reasoning behind not raising the rating to "favorable" is that any use of biological weapons would likely be seen as a failure to prevent such an attack from occurring.

If the United States puts forth a high level of effort and there is a small-scale attack, the outcome from the U.S. perspective would be

"neutral favorable." This is assuming the high level of effort has resulted in a system that is successful in monitoring and detecting the attack, that the response and recovery assets perform appropriately, and that there are few casualties. Of course, it is hard to imagine any conditions in which there was a BW attack on the United States that we would consider to have a "favorable" outcome.

The final strategy from the traditional terrorist's perspective is a large-scale attack. An implicit assumption is that a large-scale attack is not directed against a point target such as a military base, but rather is an area attack that indiscriminately affects a mix of military, governmental, and civilian targets. Based on the concern discussed previously about a traditional terrorist desire to gain and maintain support for his cause, a large-scale attack with significant casualties, including civilians, would likely be perceived as uniformly "negative." Additionally, such an attack would most likely result in a significant retribution that could become an existential threat to the traditional terrorist.

From the U.S. perspective, any large-scale attack would be considered almost uniformly "negative" because it would mean that we had failed to detect, deter, and preempt the BW threat. Only where the United States undertook a high level of effort could one remotely consider the outcome as "neutral," and only then if the U.S. response and recovery had been highly effective and casualties extremely low.

We will not go through the same exhaustive analysis for the waning and apocalyptic terrorists. The graphical assessment and some conclusions are worthy of discussion, however. Figure 4–5 provides the payoff matrix.

In the case of the waning terrorist, the only action he can take that results in a "favorable" outcome from his perspective is divestiture of all BW capabilities and intentions. This could include public denouncements of WMDs including BW, as well as divestiture of all developed capabilities. From the U.S. perspective, any outcome that would result in a waning terrorist demonstrating interest in or conducting an attack (either small scale or large scale) would have to be assessed as uniformly "negative." Only the portion of the payoff matrix where the United States makes a low level of effort and the waning terrorist divests of BW capabilities and intentions would be assessed as resulting in a "favorable" outcome. This would be seen as a prudent investment. For the United States, the higher the expenditure, the more effort is "wasted" guarding against the nonexistent threat posed by waning terrorists. Of course, this concept of waste is subjective: many would argue that efforts to improve biosurveillance and therefore prepare for a manufactured or natural biological event could be

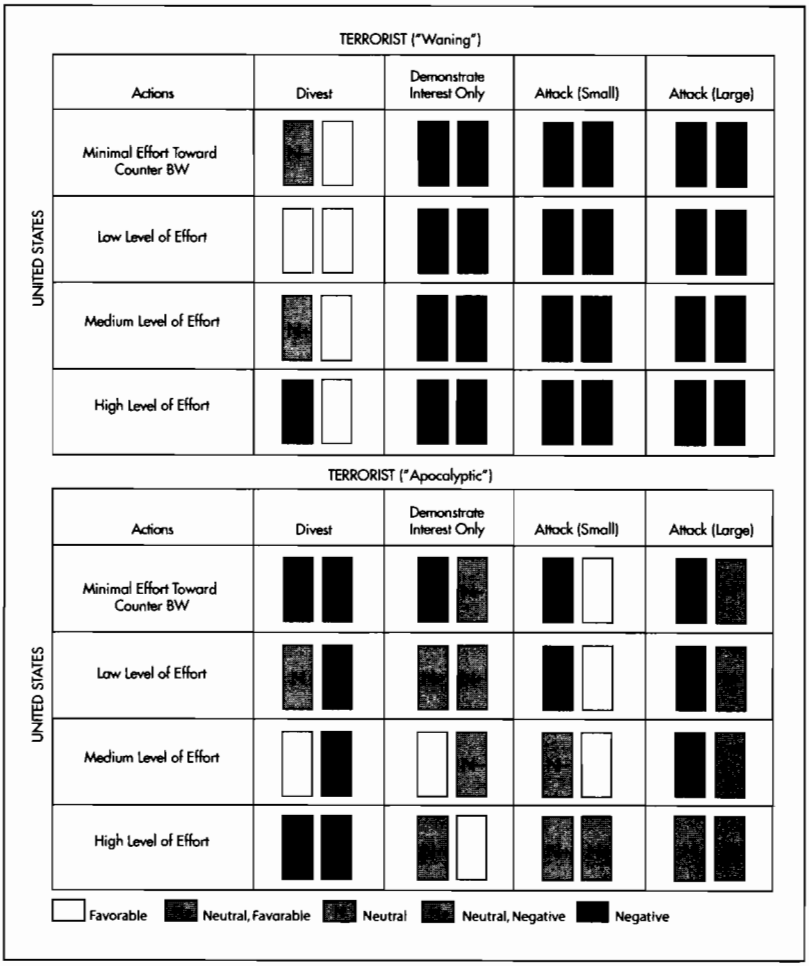


FIGURE 4–5 Payoff Matrix for the Waning and Apocalyptic Terrorists' BW Capabilities

considered resources well spent. Still, for our game we will consider these expenditures to be excessive and therefore imprudent.

In the case of the apocalyptic terrorist, the strategy employed by the waning terrorist is inverted. It is through an attack that the apocalyptic terrorist begins to achieve his goals. Divesting is therefore seen as a "negative" outcome. Demonstrating interest only is seen as "neutral-negative" for all strategies except where the U.S. put forth a high level of expenditure which would be seen as "favorable," as more resources would have been expended that were excessive and not commensurate with the threat. For the small-scale attack category, the greater the success of the

attack, the more "favorable" the perceived outcome. Only in the case of a high level of effort by the United States does the assessment change to "neutral favorable." In the case of a large-scale attack, the payoff matrix depicts a "neutral" rather than "favorable" outcome because the assessment adjusts for the difficulties associated with a small, insular group attempting to conduct a successful large-scale attack. Almost by definition, the apocalyptic terrorist would encounter more technical and operational challenges in perpetrating the larger attack.

From the U.S. perspective, spending levels need to be perceived as commensurate with the threat. In the case of the apocalyptic terrorist divesting of BW or demonstrating interest only, the United States resourcing at the medium level is the most favorable. For the small-scale attack, the outcome would be considered "negative" for the minimal and low levels and "neutral negative" for the medium level of effort, assuming a robust response and recovery. Using the same philosophy as previously discussed, any large-scale attack could not be considered "favorable" from the U.S. perspective because, once again, an attack of this magnitude would imply there was a failure to deter, dissuade, prevent, and protect the populace from such an event. Therefore, the assessment for the large-scale attack would be at best "neutral" at the high level of effort from the U.S. perspective, again assuming a vigorous response and recovery.

The discussion of game theory with regard to BW terrorism is useful for working through the motivations of the terrorists and the potential for engaging to successfully eliminate terrorist BW programs, deter and dissuade attacks, monitor the environment, respond, and recover. However, one must be mindful that terrorism is a "low-probability, high-consequence" event. Predicting terrorist attacks and understanding intentions will always be problematic because the number of variables is virtually infinite: where to attack, the means to use, the time to attack, and so on. This is why the Los Alamos analysis, which became the basis for the DHS Bioterrorism Risk Assessment, needed to consider 35 million discrete scenarios to examine the range of outcomes across the twenty-two pathogens they considered.

In the analysis of the potential for a bioterrorist attack, the most likely scenario is an attack by a traditional terrorist rather than by a waning or apocalyptic terrorist. This assertion is made for several reasons. First, most terrorists fall into the category of traditional terrorists, and groups within this category would have a propensity toward the use of violent techniques if assessed to be within their interests. Conversely, the waning terrorist would tend away from the use of violence and certainly

would tend away from the use of BW. Also, the number of terrorists in this category is comparatively small. Likewise, for the apocalyptic terrorists, while they would likely follow high-violence strategies, the number of this type of terrorist is small, making an attack from one of these terrorists extremely unlikely.

Second, the insular nature of the apocalyptic terrorist mandates a smaller cell with less outside interaction and therefore less reach for developing a complex BW capacity. It does not mean developing these capabilities will be impossible for the apocalyptic terrorist. Instead, it means the probability of success diminishes for this group. Additionally, such a group would have a more difficult time conducting a large-scale attack such as the scenario posited as part of the Atlantic Storm exercise, which considered a simultaneous release of smallpox in six locations.

The analysis described above has an important artificiality that must be noted. The world of terrorism is highly complex, with three types of terrorists existing simultaneously. In our analysis, we have considered each type in isolation. In looking at the likelihood of the outcomes, we find the traditional terrorist outcome is by far the most likely to consider for planning purposes. The waning and apocalyptic each have extremely low probabilities of occurrence. Therefore, given the numbers of apocalyptic terrorists and the motivations of the waning terrorist, we can essentially approximate the payoff analysis across all terrorists using the traditional actor payoff matrix.

In thinking about the payoff outcomes we have developed, another useful question is whether an equilibrium point exists. In game theory, such a point is called the Nash Equilibrium, a solution concept developed by John Forbes Nash. The Nash Equilibrium describes a point at which each player is assumed to know the equilibrium strategies of the other players, and no player has anything to gain by changing his own strategy (i.e., changing unilaterally). Therefore, at Nash Equilibrium each player is making the best decision he or she can, taking into account the decisions of the others. Of note, this point does not necessarily mean the best cumulative payoff for all players involved.

For our analysis, and using the payoff matrix from the traditional terrorist, we observe an apparent equilibrium point at the intersection of the U.S. medium level of effort and the terrorist demonstrating interest only. To explain this further, consider that the strategy of the United States is essentially known through policies, programs, and funding levels, and that it corresponds approximately to the medium level of effort. Of course, some elements of our programs, such as classified aspects of our efforts,

are not necessarily known. Likewise, we know from history some terrorists have demonstrated interest in BW, but we also know (as they surely have assessed) a WMD attack introduces an extremely high degree of risk with potentially existential ramifications for the terrorists. Therefore, in considering the Nash Equilibrium for our analysis, the intersection of the U.S. medium level of effort and terrorists demonstrating interest appears to define a point at which the risk and rewards are in balance and the players have little to gain by changing their respective strategies.

Just as with the previous methodology, the author would like to stress the outcomes are less important to the findings than the use of a structured methodology for examining the actions-counteractions of terrorists and U.S. policy makers. Obviously, the assessments depicted are highly sensitive to the timeframes considered, changes in the security environment, and biotechnology developments.

Previously, in looking at what history had taught us about the potential for a terrorist BW attack, a diagram was introduced. Figure 4–2 depicted the probability of a viable attack as a function of the capabilities and intentions of the terrorist. In addition, we stated that knowledge was a critical factor in any "viable attack" and that the capabilities and intentions of the terrorists were integral to the manner in which the five-step model developed previously could be used.

Figure 4–6 has been modified in several ways. The y-axis now depicts the probability of a success rather than viability of the attack. The function has been modified to depict the capabilities and intentions of the terrorists as well as our ability to prevent, protect, respond, and recover (P/P/R/R, in the equation). In this way, the graph becomes a two-sided depiction of the probability of a successful terrorist BW attack. Added to the figure is the concept of security strategies that can be brought to bear to affect the likelihood of a successful attack.

The elliptical figure is meant to reflect the trends in biotechnology in which increasingly more-critical capabilities are proliferating and becoming readily available, coupled with the trends in (1) *globalization*, where more people are gaining access to knowledge and information as well as developing the propensity for disenfranchisement and ultimately for conflict to resolve issues, and (2) *terrorism*, where we have observed a propensity toward more attacks, a higher level of violence, and more-spectacular means to perpetrate the attacks.

We have previously presented the idea of a two-sided analysis that compared the five steps required for terrorists to develop a BW capability (acquire, process, weaponize, develop scenario, and deploy) with the

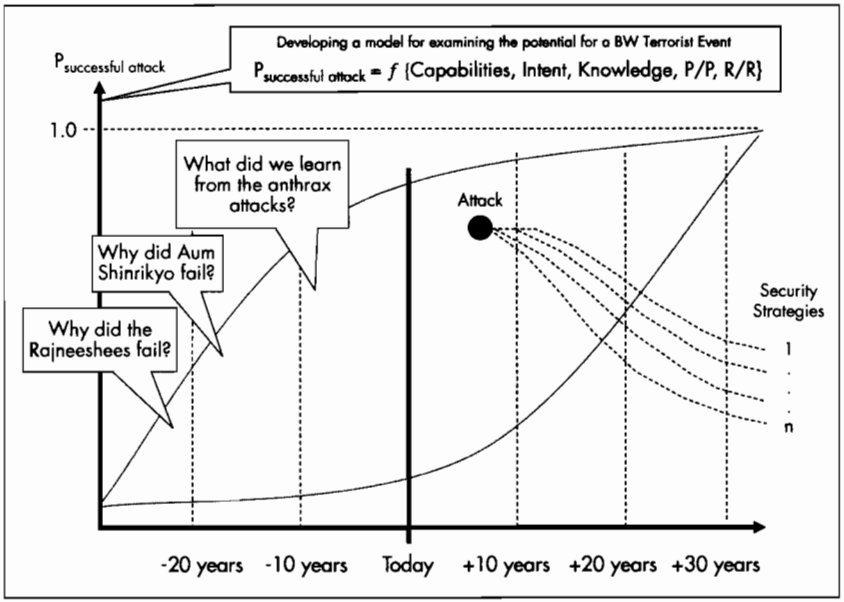


FIGURE 4-6 Examination of the Potential for a Successful Bioterror Attack

homeland security doctrine's four components (prevent, protect, respond, and recover). The relationship between these two frameworks provides an interesting opportunity to further analyze the potential for a bioterror attack and isolate the major factors that will likely determine success or failure, should an attack be launched.

The concept of using a probabilistic approach has been discussed previously, most notably in the discussion of the Los Alamos model in Chapter 2. For our purposes, we are interested in examining the individual terms of the probabilistic equation to gain an appreciation for the policy implications.

Conducting a successful bioterror attack is based on the probability of the terrorist to develop BW capabilities and successfully launch an attack and our opposing capacity to negatively influence and limit such an attack scenario, or if this fails, to respond and recover quickly. Reducing this to a probabilistic outcome expressed as the product of probabilities yields the following equation:

$$P_{Success} = [(P_{Capabilities} * P_{Intentions}) * P_{Knowledge}] * [(1 - P_{P/P/R/R})]$$

where

Probability of a Successful Attack = $P_{Success}$
Probability of a Terrorist Attaining Capabilities
(Acquisition, Processing, Weaponizing) = $P_{Capabilities}$
Probability of a Terrorist Having the Intentions
(Scenario Development and Deployment) = $P_{Intentions}$
Probability of a Terrorist Having the Knowledge = $P_{Knowledge}$
Probability of a Successfully Prevention, Protection, Response, and Recovery = $P_{P/P/R/R}$

This equation can further be expressed in its component parts, written as,

$$P_{Success} = [(P_A * P_P * P_W * P_S * P_D) * P_K] * [(1 - P_{PRE}) * (1 - P_{PRO}) * (1 - P_{RES}) * (1 - P_{REC})]$$

Due to the proliferation of biotechnology and the knowledge in this field, we must assess that the U.S. government's ability to positively affect the likelihood of either attaining the technical capabilities ($P_{Capabilities}$) or knowledge ($P_{Knowledge}$) is becoming extremely limited. Of course, this assessment is highly pathogen dependent, meaning it will remain either too difficult to acquire the necessary seed stock of certain pathogens or it will be beyond the capacity of a terrorist to process or weaponize certain pathogens. Therefore, the best opportunity to influence terrorist actions with regard to BW is to focus on the intentions represented by the term $P_{Intentions}$.

Turning to the right-hand side of the equation—the part we can influence directly through our efforts—we see a similar analysis. The ability to prevent a terrorist from acquiring, processing, and weaponizing a BW weapon is limited, and tends toward zero. One can see that as the probability of preventing a terrorist (P_{PRE}) from developing these technical capabilities approaches zero, the term $(1 - P_{PRE})$ goes to 1, meaning there is little significant prevention counterweight that can be employed.

We do have a greater capability to protect (P_{PRO}), although this too will become more challenging as the nexus between globalization, terrorism, and biotechnology continues to provide an increasing capability to the terrorists and a greater number of potential threat scenarios and possible targets to protect.

As we have discussed, we have significant ability to develop robust response and recovery programs. Therefore, the probability of a successful response and recovery—P_{RES} and P_{REC}, respectively—will be influenced directly by our actions.

Given trends in proliferation of biotech capabilities and information, and projecting toward the 2020–30 timeframe, the equation for the probability of success for the terrorist can be rewritten as follows:

$$P_{Success} = [(P_S * P_D)] * [(1 - P_{PRO}) * (1 - P_{RES}) * (1 - P_{REC})]$$

In this equation, the terms that begin to approach 1.0 (a near certainty of occurring) have been removed from the left-hand side of the equation, leaving only those that can be affected, or the scenario development and deployment aspects of terrorists actions integral to intent. Likewise, the terms with a probability approaching 0 (in this case, P_{PRE}) in the right-hand side of the equation have been allowed go to this asymptotic level as well. In this way, we are able to isolate and focus on only those terms we expect will be important in the 2020–30 timeframe while eliminating those we probably will not have the capacity to influence.

The policy implications of this revised equation are quite interesting: they imply efforts must be focused on influencing terrorists' intentions with regard to BW, rather than on significant additional efforts for preventing terrorists from developing and acquiring these capabilities. Actions taken to influence intentions—such as making clear that any bioterror act will be considered a cause for unequivocal and massive retaliation against the perpetrators—must form a basis for our future strategy. In this way, we must place at great risk anything terrorists hold dear. Taking this a step further, this must become a global strategy designed to make BW an abhorrent tactic that civilized people will not tolerate and make clear that all nations will cooperate unequivocally should such an attack be perpetrated. In this way, the threshold becomes absolute.

This discussion is not meant to imply efforts, including the AG or the Proliferation Security Imitative (PSI), should be discontinued. Rather, we must recognize the severe limitations inherent in attempting to control the proliferation of these types of technologies.

In turning to the counterweights, including protection, response, and recovery, we must recognize that policies, procedures, training, and education will be extremely important to our efforts. Sensors and standoff measures have an important role, but will not prove sufficient in reducing the probability of a successful bioterror attack. Enhanced biosurveillance that reduces the time between the first cases and a definitive determination that an attack has occurred must be the highest propriety. Additionally, technology will eventually lead to designer antibiotics and antivirals with dramatic implications for

treating exposed individuals. Until these enhanced drugs are available, a significant window of vulnerability will exist.

The message to be conveyed is that trends in globalization, terrorism, and biotechnology all point toward an increase in the propensity for a successful attack and that actions taken by the United States to reduce these vulnerabilities within the framework of national (including homeland) security will be important for reducing the likelihood of a successful bioterror attack.

An in-depth analysis of the strategies for mitigating potential terrorist BW attacks is well beyond the scope of this analysis, but some important conclusions emerge that warrant reiteration by way of a summary of this chapter.

- The threshold for terrorists to successfully develop biological weapons has been greatly reduced by trends in biotechnology and globalization. We can expect these trends to continue for the foreseeable future.
- A terrorist BW program does not require the same amount of rigor as a state program. Several events and studies combine to conclude terrorists will be able to gain BW capabilities in the future, if they do not have them already.
- The BWC, which does little with regard to tangibly eliminating state programs, is even less effective against terrorist programs. Other nonproliferation efforts such as those by the AG or the PSI face similar challenges in attempting to moderate against these types of programs.
- A potential bioterrorist will not have access to the full range of capabilities (i.e., all pathogens, contagious biological material, and so on), but likely would be able to develop a viable BW capability and perpetrate an attack. In this regard, a small-scale attack is far more likely than a large-scale attack. These probabilities will continue to increase based on globalization and biotechnology proliferation.
- International norms that moderate state behavior by deterring and dissuading states from acquiring and employing biological weapons must be used to deter and dissuade terrorists by convincing would-be bioterror perpetrators they would lose support from their constituents if they use BW. Another important strategy in this regard is to convince the potential bioterrorist the use of these capabilities would represent an existential threat.

Our game theory analysis indicates the strongest position from both the perspective of the United States and the terrorists with regard to BW is for the United States to continue to develop affordable, full-range capabilities to limit terrorist BW capability and for terrorists to continue to demonstrate interest in these capabilities, without acquiring or employing them. An attack introduces risk for the terrorist because the potential for a loss of support from their constituents and the possibility that any type of attack could become an existential threat to the group that perpetrated such an attack.