Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
CHAPTER 14

Future Directions for Biosecurity

*Nothing in life is to be feared. It is only to be understood.*

Marie Curie

Objectives

The study of this chapter will enable you to:

1. Discuss how the future of biosecurity relates to advancements in biotechnology.
2. List and describe scientific methods that may lead to the advancement of more deadly bioweapons.
3. Discuss new strategies for prevention, preparedness, and containment.

INTRODUCTION

Biosecurity has become an essential element of national security for many developed countries. Sophisticated biodefense programs have grown beyond protecting deployed military forces and have become part of homeland defense. The importance of agriculture and the threat of emerging diseases have given rise to the emergence of biosecurity systems and containment strategies that serve to protect crops, livestock, and human populations from the threat of foreign disease agents. These systems and containment strategies have taken years to develop and are likely to become more comprehensive and prominent as the future unfolds.

When looking back on the topic of biosecurity, we appreciate that many of the concerns we had came from the possibility that harmful biological agents had fallen into the wrong hands. Indeed, the technological advances in biowarfare from the Cold War era have already been used against us (Miller et al., 2002). The recent experience with anthrax-laced letters is indicative of this, but what does that portend? Might there be a more spectacular event in our near future? The author believes that the future of biosecurity will be dictated by advances in dual-use research and limited outbreaks due to emerging and reemerging disease threats.

Looking toward the future, it is clear that as the power of biological science and technology continues to grow, it will become increasingly possible that we may face an attack with a pathogen that has been deliberately engineered for increased virulence. This enhanced virulence could take the form of resistance to antibiotic drugs, increased
infectiousness (pathogenicity), or a new virulent pathogen made by combining genes from more than one organism. Threats arising from deliberate human action are not the only dangers we confront because naturally occurring infectious diseases emerge or reemerge on a regular basis (Garrett, 1995). Current examples of this include the emergence of bird flu due to H5N1 avian influenza virus and swine flu due to nH1N1, which led to a mild pandemic in 2009–2011 (see Fig. 14.1). The pathogen emerged in 1997 and, in a 10-year period, was responsible for the culling of nearly 300 million birds and more than 200 associated human deaths. The disease emerged in Hong Kong but, in the course of 10 years, spread across Asia and into Africa and Europe. Most human deaths reported have come from Cambodia, Indonesia, Thailand, and Vietnam. There have been two likely small clusters of human-to-human transmission of the H5N1 virus, and it is possible that other such transmissions have occurred. It is also possible that the H5N1 virus, through genetic mutation or recombination with a human-adapted influenza virus, could become easily transmissible among people. Given the poor condition of public health systems in many underdeveloped regions and the speed of modern air travel, the consequences of such an event would be severe. However, biosecurity

Figure 14.1 This digitally colorized transmission electron micrograph depicts numbers of nH1N1 influenza virus particles. Surface proteins located on the surface of the virus particles are shown in black. This particular strain led to a mild pandemic of swine flu in 2009–11. Courtesy of the National Institute of Allergy and Infectious Diseases.
programs sponsored by the World Health Organization and its partners, including the Centers for Disease Control and Prevention, have managed to bring sufficient attention and resources to the problem that a pandemic may have been averted. When public health strategies and biosecurity programs are successful, it is hard to know just how far the problem may have gone without intervention. The world certainly did not benefit from such programs, modern day technologies, containment strategies, and surveillance infrastructure when the 1918 Spanish flu circled the globe, leaving an estimated 40 million people dead in its wake.

With respect to dual-use research, genetic engineering is becoming routine and commonplace. Molecular genetics, genomic sequencing, and gene splicing therapies have dual-use potential. Paradoxically, the same biotechnology for developing a new drug or new vaccine may be used to develop more virulent biological weapons. As such, science that can be used to save lives may also be used to take lives (Ainscough, 2002). An outbreak of a biologically engineered pathogen might have greater disease potential than recently discovered naturally emerging diseases. A terrorist attack with a biologically engineered agent may unfold unlike any previous event. The pathogen may be released covertly, so there will be a delay between exposure and onset of symptoms. Days to weeks later, when people do develop symptoms, they could immediately start spreading contagious diseases. By that time, many people will likely be hundreds of miles away from where they were originally exposed, possibly at multiple international sites. Acutely ill victims may present themselves in large numbers to emergency rooms and other medical treatment facilities (Ainscough, 2002).

**Michael Ainscough on Future Wars**

> The 20th century was dominated by physics, but recent breakthroughs indicate that the next 100 years likely will be “the Biological Century.” There are those who say: “the First World War was chemical; the Second World War was nuclear; and that the Third World War—God forbid—will be biological.”

*Michael J. Ainscough*

In 1960 the US government formed a secret group of academic scientists, the Jason Group, to advise senior officials and help them find solutions to particularly difficult technical problems, mostly having to do with defense (Finkbeiner, 2006). In 1997 this group addressed the problem of next-generation bioweapons threats (Block, 1999). The report they produced explored a wide range of possibilities open to genetically engineered pathogens, including some that could be achieved with current state-of-the-art techniques and others that would be realized in the near future. The prospects for future bioweaponry advanced by technology are sobering (Block, 1999). In fact, technology over the past 20 years enabled scientists to engineer pathogens to be qualitatively different from conventional bioweapon agents. In terms of bioweaponry, this includes the ability to give these
“classic” pathogens attributes that might make them safer to handle, more virulent, more transmissible, harder to detect, and easier to disseminate (Block, 1999).

In their 1997 report, several broad classes of unconventional pathogens were identified by the Jason Group (Block, 1999). These include binary bioweapons, which are two-component systems that are relatively safe to handle but become deadly when the two components come together on deployment. The same technology has been used with chemical weapon systems. The Jason Group also postulated the existence of designer genes, in which specific unnatural gene sequences are built into viruses or other life forms to incorporate into the genome of the unsuspecting host, which later becomes the victim. On a similar note, they suggested that, once gene therapy becomes a medical reality, the technology that should one day allow medicine to repair or replace defective genes in a diseased individual might be subverted to introduce pathogenic sequences into healthy individuals. In addition, stealth viruses could be fashioned by a researcher to infect the host but remain silent until activated by some physiological or environmental trigger. New zoonotic agents, referred to by the Jason Group as host-swapping diseases, might be developed specifically for bio-weapon purposes by modifying existing pathogens to seek human hosts. Finally, detailed knowledge of biochemical signaling pathways could conceivably be used to create designer diseases.

Soviet Superbugs

For the most part these possibilities were actually stark realities of what some bioweapons experts refer to as the Soviet Superbug program. As discussed in chapter Seeds of Destruction, while the United States and her allies were dismantling their bioweapons programs in the 1970s, the Soviets, under Biopreparat, were assembling a huge bioweapons production capacity, comprising dozens of production facilities and as many as 60,000 personnel. This massive program aimed to build offensive capabilities by mass producing many of the Category A and B agents. More important, the Soviet bioweapons program also created research institutions with top secret goals and objectives to use biotechnology toward creating pathogens and toxins with superior capability. As we know now, the Soviets were producing Bacillus anthracis spores by the ton. We know that Soviet strains of B. anthracis were engineered to carry a form of antibiotic resistance; however, we did not know whether the North Atlantic Treaty Organization conventional anthrax vaccine was effective against all Soviet variants. Ken Alibek, a former high-ranking official in the Soviet bioweapons program, testified in 1998 before the US Congress (Alibek, 1998). Here is a chilling excerpt of what he had to say:

It is important to note that, in the Soviet’s view, the best biological agents were those for which there was no prevention and no cure. For those agents for which vaccines or treatment existed—such as plague, which can be treated with antibiotics—antibiotic-resistant or immunosuppressive variants were to be developed.
Another famed Soviet biowarfare expert and researcher, Dr. Sergei Popov, was interviewed by a journalist from the public television show NOVA. (An excerpt from the interview, entitled “Creating ‘Superbugs’,” can be accessed on the Internet; see NOVA, 2001.) In the interview, Popov admitted that the Soviets were producing synthetic genes to give microbes properties that they did not possess in nature. When Popov was asked by the interviewer “What would be the point of that?” he replied, “Imagine a new weapon which is difficult to diagnose initially and then which is impossible to treat with conventional antibiotics.” Popov explained that “the idea was that a new weapon has to have new and unusual properties, difficult to recognize, difficult to treat.” By his own admonition, the goal of his research program was to create a more deadly biological weapon. He briefly described the goal of Project Bonfire, which dealt with the creation and potential exploitation of antibiotic-resistant strains of bacteria. Under Project Bonfire, the Soviets were able to produce a strain of *Yersinia pestis* that was shown to be resistant to almost 10 antibiotics. Furthermore, a recombinant strain of anthrax had resistance to 10 antibiotics. In the Hunter Program, Popov explained that whole genomes of different viruses were being combined together to produce completely new hybrid viruses. They wanted to combine two microorganisms in one (e.g., a combination of encephalomyelitis virus and smallpox). This completely artificial agent would purportedly manifest as illness with new symptoms, probably with no known way to treat it. One might ask what would be the purpose and danger of this. In Popov’s own words:

*Essentially, the major feature would be a kind of surprise effect. Nobody would recognize it. Nobody would know how to deal with it. But nobody could predict the result of that kind of genetic manipulation.*

As for the term *superbug*, how does this exactly work? The concept sounds reminiscent of the legend of the Trojan horse. Popov explained the idea was to create a bacterial agent that harbored a virus. The virus would remain silent until the bacterial infection is treated. Therefore if the bacterial disease was recognized and treated with an antibiotic, there would be a release of virus. After the initial bacterial disease was completely cured, there would be an outbreak of a viral disease on top of this. According to Popov, a good example of this superbug model would be plague bacteria, which is relatively easy to treat with antibiotics, and viral encephalomyelitis inside. So, in case of biological attack, people would be treated against plague, and after that, the weakened host would manifest with a highly fatal infection affecting the brain and central nervous system. Remember that the encephalitides are normally transmitted by arthropod vectors, making them unlikely candidates and impractical for biowarfare. In the superbug model, the need for a vector is eliminated. Regardless, imagine the insidious nature of this scenario and the resultant fear, panic, social disruption, medical management issues, and implications for public health.
Critical Thinking

Biotechnology today is capable of most of the possibilities about which the Jason Group warned us. Some genetically engineered agents may have already been produced and stockpiled by bioweapons experts in the former Soviet Union. Consider these scenarios or possibilities:

- What if an agent could be developed that specifically targeted one or another population group? Or, what if some group could be protected against infection in advance?
- What if one could engineer a viral disease with the lethality of a hemorrhagic fever virus but the communicability of influenza?
- What if a highly lethal disease such as smallpox was hard to diagnose because it did not form pustules?
- What if a pathogen was designed to give a false-negative result on a gold standard diagnostic assay?
- What if a highly lethal pathogen with a short incubation period had never even been encountered before? How long would it take public health officials to develop a new diagnostic test and write a case definition?
- What if some pathogen could produce a localized outbreak then render itself harmless? Conversely, what if a pathogen could continually alter itself in such a way as to evade treatment?

Synthetic Biology

Concerns for the future of bioterrorism and bioweaponry remain very strong. This has been enhanced by some recent developments in what has become known as “synthetic biology.” Synthetic biology means different things to different people and groups of technical professionals. However, in the current context, the definition we will embrace here is as follows: the assemblage of natural molecules into a system that acts unnaturally. In essence, efforts in synthetic biology strive to build artificial biological systems for engineering applications using many of the same tools and experimental techniques. However, the work is fundamentally an engineering application of biological science. The focus is often on ways of taking parts of natural biological systems, characterizing and simplifying them, and using them as a component of a highly unnatural, engineered, biological system. So what is the danger in this? Imagine the construction of a microbe that can consume toxic substances (e.g., petroleum products, polychlorinated biphenyls, arsenic) to clean up the environment. Furthermore, imagine a well-funded and scientifically capable small group of terrorists perusing the scientific literature for the genomic sequencing information that enables human or animal pathogens to evade the immune system of the host, resist antimicrobial treatments, or more efficiently adhere to and invade epithelial tissues. Then imagine using this information to engineer the ultimate pathogen in a laboratory, mass produce it, and package that into a deadly bioweapon.
Critical Thinking

The “de-skilling” of molecular biology techniques coupled with genomic sequencing data access and DNA synthesis services make biology increasingly accessible to people operating outside of well-equipped professional research laboratories (Landrain et al., 2013). The emergence of do-it-yourself (DIY) biology communities has come to epitomize this supposed trend toward greater ease of access and the associated potential threat from rogue actors.

It seems that the “genie is already out of the bottle.” What can be done to mitigate the threat of unregulated laboratories conducting research using synthetic biology procedures and services?

The field of synthetic biology “aims to make biology easier to engineer” (Jefferson et al., 2014). It has also been argued that the “de-skilling” implied in synthetic biology may encourage the design of criminal bioweapons by facilitating their creation (Tucker, 2011). Such an argument relies on the idea that it would be possible to engineer pathogens without having a basic practical knowledge that is necessary in most laboratory practices. Several recent articles on this controversial subject tend to take one view or another: enhanced scientific research to be “used” for peaceful purposes or something that could be “misused”, which leads to a substantial increase in “dual-use” threats. Jefferson et al. (2014) believe that these simplistic views about synthetic biology are unwarranted and that “they embody misleading assumptions about both synthetic biology and bioterrorism.” They argue that “the importance of tacit knowledge is commonly overlooked in the dominant narrative: the focus is on access to biological materials and digital information, rather than on human practices and institutional dimensions.” They add that “public discourse on synthetic biology and biosecurity tends to portray speculative scenarios about the future as realities in the present or the near future, when this is not warranted” (Jefferson et al., 2014).

Regardless of what whether or not you believe that synthetic biology will be used by persons of groups with ill intent, we can be certain that synthetic biology has great potential. In fact, between 2008 and 2014 the US government invested more than $800 million dollars in synthetic biology research (HHS, 2014). The Department of Defense, specifically within the Defense Advanced Research Projects Agency and the Defense Threat Reduction Agency, has accounted for most of that funding. The Wilson Center completed a study in 2015 that shows that there has been very little focus on risk research with these monies. Indeed, less than 1% of the total US funding is focused on risk research and approximately 1% addresses ethical, legal, and social issues. The Wilson Center study also found that funding in other countries is rapidly increasing. In 2014 the United Kingdom and the European Commission investments in synthetic biology exceeded nondefense spending in the United States (Wilson Center, 2015). In summary, synthetic biology is a promissory field of research and an emerging technology in need of governance.
THE DARK SPECTER OF TERRORISM

It is perfectly clear to us now just how massive the Soviet bioweapons program was. After the leadership of Mikhail Gorbachev and Boris Yeltsin, bioweapons war stocks of the former Soviet Union were destroyed; much of it at one of the most remote spots on Earth, an arid island in the Aral Sea, which was formerly known to be the world’s largest biological warfare testing ground, Vozrozhdeniye Island. So what remains of the former Soviet arsenal and where are all of the seed stocks from the bioengineering efforts of Project Bonfire and the Hunter Program? Have deadly superbugs been sequestered for dark days ahead? Furthermore, what other countries have had and remain actively engaged in bioweapons production and research? The Office of the Secretary of Defense identified countries that maintain various levels of offensive biological warfare capabilities or research facilities. China, Iran, Israel, Libya, North Korea, Syria, and Taiwan are believed to have produced operational quantities of biological weapons (U.S. Congress, Office of Technology Assessment, 1993). The Henry L. Stimson Center also identified Egypt, Israel, and Taiwan as countries of proliferation concern (Block, 1999). The Al Qaeda network is reported to have sought to purchase biological agents, and some on-site reports suggest that their rudimentary laboratory facility at Tarnak Farm, Afghanistan, was being set up for biological and chemical agent production.

The technology required to mass produce biological agents (e.g., yeast, bacteria, and viruses) is relatively inexpensive. Beer, cosmetics, pharmaceuticals, and vaccine production facilities alike use much of the same equipment, making it relatively easy to acquire. If there is any doubt about this, explore the possibility of setting up your own laboratory by shopping online with one of the Internet auctioneers to see how readily available and inexpensive laboratory equipment and fermentation chambers are. Most microbial agents needed for biological weapons may be naturally sourced. “It is difficult to gauge the extent of biological weapons development in other nations since production facilities require little space and are not easy to identify. The acquisition and dissemination of even the most highly restricted organism, Variola major, is not an implausible scenario” (Inglesby et al., 2000).

In the age of terrorism, our adversaries no longer wear uniforms and fight us on a battlefield with clearly defined boundaries and objectives. The threat is now asymmetric, and as such, biological weapons will always be an option. Belligerents, allured by the potentially deadly power of weapons of mass destruction, strive to acquire them (Ainscough, 2002). However, when biological weapons have been used in battle, they have proven relatively ineffective. They have been undependable and uncontrollable (Zilinskas, 2000). Because they have been difficult to reliably deploy, their military value has been marginal. Stabilizing biological agents and deploying them, either overtly with sophisticated weaponry or covertly without endangering the perpetrator
or friendly forces, requires expertise not widely held (Ainscough, 2002). It is possible that this may change with the capabilities of biological engineering and a new generation of weapons.

**Critical Thinking: Possible Future Bioweapons Scenarios**

Dr. Jim Davis (2002) stated that the three most likely bioweapons scenarios that the United States and its allies might face in the future are the following:

- An agroterrorist event against the United States,
- A bioweapons attack on US and allied troops in the Middle East, and
- A bioterrorist attack against a large population center in the United States or an allied state.

On the basis of what you know now and the current world situation, are these three possibilities still valid? What has changed since 2002 to make these three scenarios more or less likely?

Well-developed militaries are trained and equipped to operate in chemical and biological environments. Vulnerable civilian populations have neither the protective equipment nor defensive training; therefore they are totally unprepared for a biological attack. Naturally, these civilian populations are the most likely “soft” target for a bioterrorist objective. According to Sprinzak (2001), the “megalomaniacal hyperterrorists” of the modern era are innovative and resourceful. They are always looking for ways to surprise and devastate the enemy. They think big, seeking to go beyond “conventional” terrorism, and unlike most terrorists, they could be willing to use weapons of mass destruction. If the intent of terrorists is to inflict mass casualties, then biological agents are likely to be used (Ainscough, 2002).

**Biological Warfare**

Nuclear warfare threat has been one of the main driving forces for cultural, political, economical and social changes in the late twentieth century. Biological warfare threat is about to take over. However, while nuclear warfare was a concrete possibility, biological warfare is just an elusive risk.

*Emilio Mordini (2005)*

Bioweapons counterproliferation expert Dr. Jim Davis stated there are at least six reasons why senior officials and skeptics believe a significant bioweapons attack will not occur (Davis, 2002). These reasons, which he characterizes as myths and false assumptions, are as follows:

**Myth 1. There never really has been a significant bioweapons attack.**
Counter: From our readings in chapter *Seeds of Destruction*, we know this is not true.

**Myth 2. The United States has never been attacked by a bioweapons agent.**
Counter: Consider Amerithrax and the Rajneeshee incident as significant bioweapons attacks on US soil.
Myth 3. **You have to be extremely intelligent, highly educated, and well funded to grow, weaponize, and deploy a bioweapons agent.** Counter: If you can source the agent and know something about the fermentation processes, then you can make a crude but effective agent concoction. Terrorist groups with relatively few resources and a lot of “want to” could manage to pull together a bioweapons attack. In addition, a small group with connections may be able to procure a small amount of formulated material, which may be enough to introduce a disease with a high degree of person-to-person transmissibility.

Myth 4. **Biological warfare must be too difficult because, when it has been tried, it has failed.** Counter: There are certainly those that would argue Aum Shinrikyo’s blunder with anthrax is an indication that well-funded terrorism is no guarantee for success. On many fronts, evildoing is not easy. However, that is no guarantee that subsequent attempts would not be successful. It only takes one successful attempt to make the point that it is easier to prepare for bioterrorism than to explain the lack of preparation after an attack.

Myth 5. **There are moral restraints that have and will keep bioweapons agents from being used.** Counter: If a terrorist can fly a jumbo jet into a high-rise office building filled with thousands of innocent people, there really are no moral boundaries when it comes to terrorism.

Myth 6. **The long incubation period required for bioweapons agents before onset of symptoms makes bioweapons useless to users.** Counter: Do not make the mistake of questioning the motives or means of a terrorist. A long incubation period may work to someone’s advantage, especially if the act is covert and the perpetrator is looking to disseminate the agent along a broad front or from numerous points of release to make containment more difficult.

**STRATEGIES FOR PREVENTION, PREPAREDNESS, AND CONTAINMENT**

Hospitals will bear the brunt of caring for the sick and dying should a biological weapon be used. However, few hospitals are prepared to cope with even a handful of cases of a highly contagious, life-threatening disease, and few hospitals are prepared to manage even a modest surge in the numbers of seriously ill patients. Hospital leaders should examine current policies in relation to this threat and develop new policies as appropriate. Infection control practices are but one critical component of such planning efforts (Inglesby et al., 2000). As previously discussed in chapters Recognize, Avoid, Isolate, and Notify and Response at the State and Local Level, response organizations and community officials have increased their awareness to this threat, but it remains one of the least understood. Much more effort along these lines to heighten awareness and bolster surveillance is needed. We cannot allow this relative period of quiescence after Amerithrax to lull us into a state of ill preparedness.
Homeland Security Presidential Directive 18, released in early 2007, outlines strategies for medical countermeasure research, development, and acquisition, and it frames the spectrum of biological threats in four distinct categories:

- **Traditional agents.** Naturally occurring microorganisms or toxin products with the potential to be disseminated to cause mass casualties. Examples include *B. anthracis* (anthrax) and *Y. pestis* (plague).

- **Enhanced agents.** Traditional agents that have been modified or selected to enhance their ability to harm human populations or circumvent available countermeasures. Examples include drug-resistant pathogens such as extensively drug-resistant tuberculosis (see Fig. 14.2) or multidrug-resistant plague.

- **Emerging agents.** Previously unrecognized pathogens that might be naturally occurring and present a serious risk to human populations. Tools to detect and treat these agents might not exist or be widely available. An example is severe acute respiratory syndrome or bird flu (avian influenza).

- **Advanced agents.** Novel pathogens or other biological materials that have been artificially engineered in the laboratory to bypass traditional countermeasures or produce a more severe or otherwise enhanced spectrum of disease. An example is multidrug-resistant anthrax.

![Figure 14.2](image-url) This scanning electron micrograph depicts numerous clumps of methicillin-resistant *Staphylococcus aureus* bacteria, commonly referred to as MRSA, magnified 9560 times. Recently recognized outbreaks, or clusters, of MRSA in community settings have been associated with strains that have some unique microbiologic and genetic properties compared with the traditional hospital-based MRSA strains, which suggests that some biologic properties (e.g., virulence factors such as toxins) may allow the community strains to spread more easily or cause more skin disease. Antibiotic-resistant bacteria, such as MRSA, and drug-resistant strains of *Mycobacterium tuberculosis* (the etiologic agent of tuberculosis), will become increasingly important in public health and infection control settings. There is also the potential that they may be exploited because of the difficulty of control. *Courtesy of the Centers for Disease Control Public Health Image Library.*
These designations expand on the traditional classifications of Category A, B, and C agents because they address the fact that future threats are likely to be unanticipated and ill defined. Although appropriate and effective for the highest priority traditional threats, such as smallpox and anthrax, developing medical countermeasures using a conventional “one bug–one drug” approach will rapidly prove unsustainable as the list of threats increases to include enhanced, emerging, and advanced agents. Responding to traditional and new types of threats requires the capability to rapidly identify unknown or poorly defined agents, quickly evaluate the efficacy of available interventions, and develop and deploy novel treatments to prevent or mitigate medical consequences and the subsequent impact on society. It is certain that the importance of the Laboratory Response Network and the establishment of regional centers of excellence for biodefense and emerging infectious diseases have been realized (see Fig. 14.3). Maintaining this vital capability to guide recognition of the threat is costly but essential.

THE FUTURE OF BIODEFENSE RESEARCH

Scientific research for biodefense is constantly needed to identify new diagnoses, prevention, or treatment for infectious disease. Commensurate with this, the infectious diseases community might elect to encourage and reward basic science research efforts that seek to produce novel diagnostic technologies and preventive or therapeutic interventions for the diseases caused by biological weapons. That agenda was successfully outlined in 2005 by Dr. Anthony Fauci, Director of the National Institutes of Health (Fauci, 2005).

Developing medical countermeasures against a finite number of known or anticipated agents is a sound approach for mitigating the most catastrophic biological threats. However, responding to enhanced, emerging, and advanced agents demands new paradigms, which allow for more rapid and cost-effective development of countermeasures. The National Institutes of Health, in collaboration with other agencies, established a solid framework of research and product development resources for biodefense. The program, outlined in 2007, called for new approaches to provide the flexibility required to meet the challenges of nontraditional threats. The National Institute for Allergy and Infectious Diseases (2007) identified three “broad-spectrum” strategies to create a more responsive biodefense capability (see Fig. 14.4). These strategies remain in place and are hereafter described.

Broad-Spectrum Activity

Broad-spectrum activity is a characteristic that enables a particular product to mitigate biological threats across a wide range or class of agents. Multiplex diagnostics possessing broad-spectrum activity rapidly differentiate various common and lesser-known pathogens in a single clinical sample, identify drug sensitivities, and determine how a
sample pathogen is related to known pathogens. Consider the lab-on-a-chip concept, in which a clinical specimen is placed on a microchip–like device, which has a complex microarray of DNA– or ribonucleic acid (RNA)–based diagnostics. The chip allows the processing unit to test for dozens of possibilities simultaneously based on DNA– or RNA–hybridization modalities. Some exciting new developments along these lines have already occurred. Vaccines demonstrating broad-spectrum activity include cross–protective and multiple–component vaccines. Cross–protective vaccines induce an immune response against constant components of a microbe; therefore they are effective against pathogens that naturally or deliberately evolve or “drift”.

Figure 14.3  A scientist in the process of transferring specimens in one of the Centers for Disease Control biosafety level–4 laboratories, located in Atlanta, Georgia. The scientist wears a protective airtight suit equipped with a helmet and face mask. She is seated at a negatively pressurized laminar flow hood that allows no air flow to escape back into the laboratory environment. Using this negatively pressurized, hooded environment, any airborne pathogens or toxic vapors are drawn back into the hooded container and up into a filtered ventilation system, thereby avoiding the spread of contaminants through the laboratory. Although these facilities are very costly to staff and maintain, they are vital and give us the ability to investigate unknown threats and emerging diseases. Regional centers of excellence have given the United States biosafety level–4 capacity. Courtesy of the Centers for Disease Control Public Health Image Library.
A universal influenza vaccine is an example of a cross-protective vaccine. Multiple-component vaccines include, within a single vaccine, elements that protect against viruses or microbes that are different but usually closely related. An example of a multiple-component vaccine is a hemorrhagic fever vaccine that contains elements of Ebola, Marburg, and Lassa viruses.

For several traditional threats, safe and effective treatments are nonexistent, of limited usefulness, or susceptible to emerging antimicrobial resistance and genetically engineered threats. A limited number of antinfectives with broad-spectrum activity directed at common, invariable, and essential components of different classes of microbes could be effective against traditional and nontraditional threats. This approach would allow a small number of drugs to replace dozens of pathogen-specific drugs. In addition, the strategies to overcome antibacterial resistance could extend the clinical utility of existing broad-spectrum anti-infectives and have immediate benefits. Treatments that target host immune responses have the potential to be effective against multiple diseases. These immune modulators reduce morbidity and mortality by controlling responses that contribute to disease (eg, cytokine storms) or nonspecifically activating the host’s natural immune defenses to induce a faster, more potent protective response.

**Broad-Spectrum Technology**

Broad-spectrum technology refers to capabilities, such as temperature stabilization or delivery method, that can be engineered into a wide array of existing and candidate products. Developing countermeasures that will be useful in responding to future threats represents a major challenge given the capabilities that these products
must possess. They should be safe and effective against multiple pathogens in people of any age and health status. To be appropriate for storing in the Strategic National Stockpile, the products should be suitable for long-term storage at room temperature, have simple compact packaging, be easily delivered in a mass casualty setting, confer protection with limited dosing, and have single-dose delivery devices that can be self-administered. Added to these factors is the potential need to produce additional quantities with little notice, requiring manufacturers to take the costly step of keeping production facilities on standby. A recent example of this is the relatively rapid creation and production of a vaccine for H5N1 bird flu, which is already approved by the Food and Drug Administration with 5 million doses placed in the Strategic National Stockpile.

**Broad-Spectrum Platforms**

Broad-spectrum platforms are standardized methods that can be used to significantly reduce the time and cost required to bring medical countermeasures to market. For example, a proven monoclonal antibody fermentation and purification method can be applied to rapidly develop any therapeutic monoclonal antibody, avoiding lengthy development work. Other examples of platform technologies include screening systems, in vitro safety testing, expression modules, manufacturing technologies, and chemical synthesis designs. The potential to rapidly apply such platform methods to developing new countermeasures will considerably shorten and streamline the process.

**Bioweapons and Scientists**

*The community of biologists in the United States has maintained a kind of hand-wringing silence on the ethics of creating bioweapons—a reluctance to talk about it with the public, even a disbelief that it’s happening. Biological weapons are a disgrace to biology. The time has come for top biologists to assert their leadership and speak out, to take responsibility on behalf of their profession for the existence of these weapons and the means of protecting the population against them, just as leading physicists did a generation ago when nuclear weapons came along. Moral pressure costs nothing and can help; silence is unacceptable now.*

*Richard Preston (1998)*

**CONCLUSION**

It is clear that security and defense against biological threats, whether natural or the result of deliberate human action, will continue to be a high priority for the foreseeable future. Biological warfare and bioterrorism are multifaceted problems requiring multifaceted solutions (*Block, 1999*). We need our best critical thinkers and biological
researchers to solve this constantly evolving problem. Fortunately, the same advances in genomic biotechnologies that can be used to create bioweapons can also be used to set up countermeasures against them. The probability of a terrorist use of a genetically engineered biological agent on a given city is very low, but the consequence of such an event would obviously be very high. With maximum casualties the likely goals, metropolitan areas are most at risk for an attack. However, the indiscriminate nature of biological warfare and bioterrorism puts all communities at risk. This dilemma is the challenge of local communities, which are sensitive to the need for preparedness but have finite resources. Community officials must have a plan and sufficient medical and public health resources accessible to sustain a response for up to 24 h. Robust federal assistance would be made available promptly, but it would not be immediate. At present, all military and civilian populations throughout the world are vulnerable to a bioweapons attack. We remain grossly ill-prepared to respond to an epidemic caused by a novel genetically engineered biological agent.

President Nixon said it best when he stated, “Mankind already carries in its own hands too many of the seeds of its own destruction.” We know that he was forewarning us that further advances in biowarfare and the production of bioweapons could ultimately end in our own demise. Acting responsibly, he put an end to our biological weapons arsenal and focused our assets on biodefense rather than biooffense. We now have in place sophisticated and well-developed biosecurity and biodefense programs. These programs are essential to countering the asymmetric warfare threat, but they are costly and perishable. Future directions in biosecurity and biodefense may very well be determined by the “next event.” However, it is this author’s opinion that the most likely events are those that naturally and accidentally threaten human and animal health through the emergence of novel pathogens and the reemergence of others in light of new environmental or societal factors.

**ESSENTIAL TERMINOLOGY**

- **Binary bioweapons.** A two-component system consisting of innocuous parts that are mixed immediately before use to form the pathogen. This process occurs frequently in nature. Many pathogenic bacteria contain multiple plasmids (small, circular, extrachromosomal DNA fragments) that code for virulence or other special functions. Virulent plasmids can be transferred among different kinds of bacteria and often across species barriers (Block, 1999).

- **Designer diseases.** The possibility that science one day might allow a researcher to propose the symptoms of a hypothetical disease and then design or create the pathogen to produce the desired disease complex. Designer diseases may work by turning off the immune system; by inducing specific cells to multiply and divide rapidly (similar to cancer); or possibly by causing the opposite effect, such as initiating
programmed cell death (apoptosis). This futuristic biotechnology would clearly indicate an order of magnitude of advancement in offensive biological warfare or terrorism capability (Block, 1999).

- **Designer genes.** The entire genomes of numerous organisms have been published in unclassified journals and on the Internet. Now that the codes are known, it seems only a matter of time until microbiologists develop synthetic genes, synthetic viruses, or even complete new organisms. Some of these could be specifically produced for biological warfare or terrorism purposes (Block, 1999).

- **Gene therapy.** Gene therapy will revolutionize the treatment of human genetic diseases. The goal is to effect a permanent change in the genetic composition of a person by repairing or replacing a faulty gene. The same technology could be subverted to insert pathogenic genes in a targeted host of population (Block, 1999).

- **Host-swapping diseases.** Viruses that “jump species” may occasionally cause significant disease. Manageable infectious agents can be transformed naturally into organisms with markedly increased virulence (Block, 1999).

- **Stealth viruses.** The concept of a stealth virus is a cryptic viral infection that covertly enters human cells (genomes) then remains dormant for an extended time. However, a signal by an external stimulus could later trigger the virus to activate and cause disease. In fact, this mechanism occurs fairly commonly in nature. For example, many humans carry herpes virus, which can activate to cause oral or genital lesions. Similarly, varicella virus sometimes reactivates in the form of herpes zoster (shingles) in some people who had chickenpox earlier in life. However, the vast majority of viruses do not cause disease (Block, 1999).

- **Synthetic biology.** Synthetic biology is an interdisciplinary branch of biology combining disciplines such as biotechnology, evolutionary biology, molecular biology, systems biology, biophysics, computer engineering, and genetic engineering.

**DISCUSSION QUESTIONS**

- What is the most likely reason for biosecurity programs to increase in scope and complexity?
- Is a major act of bioterrorism likely in the next 5 years? If not, what will that do to existing research programs and surveillance systems such as BioWatch?
- Imagine that bioweapons programs come back into prominence and there is a renewed interest in creating superbugs in sophisticated state-sponsored programs. How could technology today give a military advantage to a country?
- What would be the likely outcome if an adversary overtly used a biological weapon against its enemy? What sort of a response would the international community pursue? Might it provoke the use of a nuclear weapon?
WEBSITES
Regional centers of excellence for biodefense and emerging infectious diseases (10 centers, located nationwide, provide resources and communication systems that can be rapidly mobilized and coordinated with regional and local systems in response to an urgent public health event). Available at: http://www.niaid.nih.gov/labsandresources/resources/rce/Pages/default.aspx.

National biocontainment laboratories (NBLs) and regional biocontainment laboratories (RBLs; 2 NBLs and 13 RBLs are available or under construction for research requiring high levels of containment and are prepared to assist national, state, and local public health efforts in the event of a bioterrorism or infectious disease emergency). Available at: http://www.niaid.nih.gov/labsandresources/resources/dmid/nbl_rbl/Pages/default.aspx.

The Biodefense and Emerging Infections Research Resources Repository (offers reagents and information essential for studying emerging infectious diseases and biological threats). Available at: https://www.beiresources.org/.

Health and Human Services. Public Health Emergency Countermeasures Enterprise Implementation and Strategic Plan (2014). Available at: http://www.phe.gov/Preparedness/mcm/phemce/Documents/2014-phemce-sip.pdf.

National Institutes of Health Biodefense Strategic Plan. Available at: http://www.niaid.nih.gov/topics/BiodefenseRelated/Biodefense/Pages/strategicplan.aspx.

REFERENCES
Ainscough, M., 2002. Next generation bioweapons: genetic and BW. In: Davis, J., Schneider, B. (Eds.), The Gathering Biological Warfare Storm. USAF Counterproliferation Center, Air War College, Air University, Maxwell Air Force Base, Montgomery, AL (Chapter 9).
Alibek, K., May 20, 1998. Terrorist and Intelligence Operations: Potential Impact on the US Economy. Statement before the Joint Economic Committee. U.S. Congress. Available at: http://fas.org/irp/congress/1998_hr/alibek.htm.
Block, S., 1999. Living nightmares: biological threats enabled by molecular biology. In: Drell, S., Sofaer, A., Wilson, G. (Eds.), The New Terror: Facing the Threat of Biological and Chemical Weapons. Hoover Institution Press, Stanford, CA, p. 60.
Davis, J., 2002. A biological warfare wake-up call: prevalent myths and likely scenarios. In: Davis, J., Schneider, B. (Eds.), The Gathering Biological Warfare Storm. USAF Counterproliferation Center. Air War College, Air University, Maxwell Air Force Base, Montgomery, AL (Chapter 10).
Fauci, A., July 28, 2005. Testimony before the Committee on Homeland Security, Subcommittee on the Prevention of Nuclear and Biological Attack United States House of Representatives by the Director of the National Institute of Allergy and Infectious Diseases. National Institutes of Health, U.S. Department of Health and Human Services.
Finkbeiner, A., 2006. The Jasons: The Secret History of Science’s Postwar Elite. Viking Books, New York.
Garrett, L., 1995. The Coming Plague: Newly Emerging Diseases in a World Out of Balance. Farrar, Straus and Giroux, New York.
Inglesby, T., O’Toole, T., Henderson, D.A., 2000. Preventing the use of biological weapons: improving response should prevention fail. Clinical Infectious Diseases 30, 926–929.
Jefferson, C., Lentzos, F., Marris, C., 2014. Synthetic biology and biosecurity: challenging the “myths”. Frontiers in Public Health 2, 115. Available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4139924/.

Landrain, T., Meyer, M., Perez, A., Sussan, R., 2013. Do-it-yourself biology: challenges and promises for an open science and technology movement. Systems and Synthetic Biology 7, 115–126.

Miller, J., Engelberg, S., Broad, W., 2002. Germs: Biological Weapons and America’s Secret War. Simon and Schuster, New York.

Mordini, E., 2005. Biowarfare as a biopolitical icon. Poiesis & Praxis: International Journal of Technology Assessment and Ethics of Science 3, 242–255.

National Institute of Allergy and Infectious Diseases, 2007. Strategic Plan for Biodefense Research. 2007 Update. U.S. Department of Health and Human Services, National Institutes of Health, Washington, DC.

NOVA, 2001. Soviet “Superbugs,” Interview between NOVA and Sergei Popov. Available at: www.pbs.org/wgbh/nova/bioterror/biow_popov.html.

Preston, R., April 21, 1998. Taming the Biological Beast. Op-Ed. New York Times.

Sprinzak, E., November–December 2001. The lone gunman. Foreign Policy 72–73.

Tucker, J., 2011. Could Terrorists Exploit Synthetic Biology? The New. Atlantis.com.

U.S. Congress, Office of Technology Assessment, 1993. Technologies Underlying Weapons of Mass Destruction. OTA-BP-ISC-115. Government Printing Office, Washington, DC.

U.S. Department of Health and Human Services, 2014. Public Health Emergency Countermeasures Enterprise Implementation and Strategic Plan. http://www.phe.gov/Preparedness/mcm/phemce/Documents/2014-phemce-sip.pdf.

Wilson Center, 2015. U.S. Trends in Synthetic Biology Research Funding, Available at: https://www.wilsoncenter.org/sites/default/files/final_web_print_sept2015_0.pdf.

Zilinskas, R., 2000. Biological Warfare: Modern Offense and Defense. Lynne Rienner Publishers, Boulder, CO.