Biosecurity:

Limiting Terrorist Access to Deadly Pathogens

Jonathan B. Tucker

United States
Institute of Peace

Peaceworks

Peaceworks No. 52. First published November 2003.

United States Institute of Peace
1200 17th Street NW, Suite 200
Washington, DC 20036-3011

Phone 202-457-1700
Fax: 202-429-6063
E-mail: usip_requests@usip.org
Web: www.usip.org

Contents

Summary

Long a hypothetical threat, bioterrorism became a harsh reality soon after September 11, 2001, when letters containing a refined preparation of dried anthrax spores were sent through the U.S. mail, infecting more than twenty people and killing five. Although the October 2001 anthrax attack was fortunately limited in scale, it hinted at the mayhem that could result from the deliberate release of "weaponized" disease agents. In this Peaceworks report, Jonathan B. Tucker, a 2002–03 Jennings Randolph Senior Fellow at the U.S. Institute of Peace, explores current national and international efforts to prevent terrorists from acquiring dangerous pathogens and argues for the establishment of a set of global biosecurity standards.

Tucker was a United Nations Special Commission (UNSCOM) biological weapons inspector in Iraq in February 1995, and he directed the Chemical and Biological Weapons Nonproliferation Program at the Monterey Institute of International Studies' Center for Nonproliferation Studies (CNS) from 1996 to 2002. He is currently a senior researcher at the CNS office in Washington, D.C. Before joining the center, he was a specialist on chemical and biological arms control at the United States Arms Control and Disarmament Agency and the congressional Office of Technology Assessment. His most recent book, *Scourge: The Once and Future Threat of Smallpox* (Atlantic Monthly Press, 2001), was selected as a "Best Book of the Year" by the *Washington Post.* During his fellowship at the U.S. Institute of Peace, Tucker researched prevention-oriented strategies for countering bioterrorism; his principal findings are presented in this Peaceworks report.

To date, most of the emphasis in countering bioterrorism has been on the medical and public health response to an attack, rather than on prevention. Tucker notes that while improved disease surveillance and medical countermeasures such as new drugs and vaccines are important, there should be an equal emphasis on reducing the risk of an attack. He begins by distinguishing between the concepts of biosafety and biosecurity. Whereas biosafety refers to measures to prevent the accidental release of pathogens, biosecurity involves measures that guard against the deliberate release of pathogens for malicious purposes; yet most national and international legislation to date has focused on biosafety and not biosecurity. In a belated effort to improve security at microbiological laboratories and biological suppliers after the September 11 terrorist attacks and the subsequent anthrax letter attacks, Congress passed two significant pieces of legislation (the USA PATRIOT Act and the Bioterrorism Preparedness Act) that tightened controls over dangerous pathogens and toxins stored, used, and transferred within the United States.

Nevertheless, according to Tucker, the international dimension of the biosecurity problem remains to be addressed. No uniform global standards for laboratory security currently exist on which individual states can base national legislation and regulations. This lack of harmonization, Tucker argues, has given rise to gaps and vulnerabilities that must be addressed as part of a coordinated global strategy to prevent bioterrorism.

The United States is just one of many countries that conduct research on infectious disease agents and maintain collections of dangerous pathogens. According to Tucker, one area of particular concern is the legacy of the Soviet offensive biological warfare program. Today, many former bioweapons-related facilities—now located in the independent states of Russia and Kazakhstan—have been converted to civilian uses. Nevertheless, they continue to possess collections of highly dangerous pathogens that could potentially be stolen or diverted for military, terrorist, or criminal purposes. Although improved security for collections of dangerous pathogens in the former Soviet Union is urgently needed, many laboratories (such as those associated with the network of Anti-Plague Institutes and field stations) lack the necessary financial and technical resources to implement these measures.

Tucker cautions that the former Soviet Union is not the only area of concern. Several countries now operate maximum-containment (Biosafety Level-4) laboratories designed for work with the most dangerous and incurable pathogens. Security risks are also associated with roughly one-third of the fifteen hundred state-owned and commercial culture collections worldwide that possess, exchange, and sell samples of microorganisms and toxins for legitimate scientific and biomedical research. Culture collections vary widely in size and content—ranging from large organizations, such as the nonprofit American Type Culture Collection in Virginia and the U.S. Department of Agriculture's collection of plant and animal pathogens in Ames, Iowa, to small "boutique" collections of microbial strains at universities, federal agencies, and private companies. Numerous culture collections outside the United States are not adequately secured and controlled, making them potentially vulnerable to theft by proliferators and terrorists. In addition, trade in microbial cultures is poorly regulated, both within and among countries.

To address this problem, several countries in addition to the United States have passed legislation concerning laboratory security. Nevertheless, Tucker argues, national biosecurity regulations must be reasonably uniform to prevent terrorists from stealing deadly pathogens from poorly protected facilities in those countries where laws or enforcement are lax. Relying exclusively on uncoordinated national standards would lead to a patchwork of regulations and create pockets of weak implementation or enforcement that terrorists could exploit as targets of opportunity. Only global biosecurity standards, Tucker believes, will place significant obstacles in their path.

Recently, a few international organizations, including the World Federation for Culture Collections, the Organization for Economic Cooperation and Development, the European Union, and health ministers from the Group of Seven plus Mexico, have launched initiatives in the biosecurity field. However, while these initiatives are useful steps in the right direction, they remain uncoordinated and incomplete. In Tucker's view, only truly global biosecurity standards will reduce the risk of terrorists obtaining dangerous pathogens from foreign sources; such standards would also facilitate collaborative research to develop protective vaccines and drugs. For this reason, Tucker argues, the international scientific community and the security community should work closely together to develop practical and cost-effective approaches to biosecurity.

Tucker offers a roadmap for the negotiation of global biosecurity standards, suggesting that they should include not only emergency response plans in case of biosecurity breaches, but also the following *preventive* elements: (1) mechanisms to account for

pathogens that are being stored, used during experiments, or transferred or exported; (2) the registration and licensing of facilities that work with dangerous pathogens; (3) physical security at these facilities; and (4) procedures for screening laboratory personnel. Model biosecurity legislation is problematic because countries have incompatible legal systems; accordingly, Tucker suggests that a technical working group be established under the auspices of the Biological Weapons Convention (BWC) to develop detailed guidelines for national legislation. In addition to representatives of BWC member states, such a group might include experts from the World Health Organization, the Food and Agriculture Organization, and the World Organization for Animal Health.

To ensure a degree of uniformity and accountability in national implementation of such voluntary standards, Tucker proposes that an international oversight mechanism be created. This mechanism, which might be coordinated by a small secretariat, would invite the participating states to submit written reports on the implementation of biosecurity standards and to attend annual meetings at which they can raise concerns about possible gaps in biosecurity in other countries and apply political pressure to ensure that such deficiencies are corrected. Tucker concludes this report by stating that the negotiation of global biosecurity standards would provide a concrete means of reducing the risk of bioterrorism while strengthening the international legal norm against the acquisition and use of biological weapons by both states and terrorist organizations.

Acknowledgments

I am grateful to the staff of the Jennings Randolph Program at the United States Institute of Peace, particularly to Joe Klaits and Ginny Bouvier, for the opportunity to research and write this report. Thanks are also due to the following experts who provided useful comments on earlier drafts: Thomas Cataldo of the U.S. Department of Defense, Gerald L. Epstein of the Defense Threat Reduction Agency, Julie E. Fischer of the Henry L. Stimson Center, Nancy Gallagher of the University of Maryland, Reynolds M. Salerno of Sandia National Laboratories, Janet Shoemaker of the American Society for Microbiology, Frank P. Simione of American Type Culture Collection, Gregory J. Stewart of the U.S. Department of State, and Mark Wheelis of the University of California, Davis. Peter Pavilionis expertly shepherded the report through the Institute publications process.

One

The Biosecurity Challenge

Bioterrorism, once a largely hypothetical threat, became a harsh reality in the fall of 2001 when letters containing a fine powder of dried anthrax spores were sent through the U.S. mail, infecting twenty-two people and killing five. Despite the fact that the attacks involved only about ten grams of powdered anthrax, the ripple effects temporarily disrupted all three branches of the federal government, closed down congressional offices and mail processing stations, and frightened millions of Americans. These far-reaching consequences hinted at mayhem that could result from the large-scale release of a "weaponized" disease agent.

The only previously known incident of bioterrorism in the United States took place in 1984, when members of the Rajneeshee cult contaminated restaurant salad bars in the town of The Dalles, Oregon, with *Salmonella*, a bacterium that causes food poisoning. The motive behind this attack was to test a scheme to incapacitate local residents temporarily, preventing them from voting in a county election and tilting the outcome in the cult's favor. Although the resulting outbreak of food poisoning sickened 751 people (some seriously), there were no fatalities.[1]

Recent evidence suggests that the threat of bioterrorism is real and growing. Documents and computer hard drives seized during the March 1, 2003, capture of Khalid Shaikh Mohammed, a key operational planner for Al Qaeda, revealed that the organization had recruited a Pakistani microbiologist, acquired materials to manufacture botulinum toxin, and developed a workable plan for anthrax production.[2]

Rapid advances in biological science and technology are also changing the nature of the bioterrorism threat. Genetic engineering has made it theoretically possible to render natural disease agents more lethal, contagious, or environmentally persistent, evade detection and diagnosis, and defeat existing drugs and vaccines. Although nuclear physicists have grappled for decades with the dark side of their discipline, awareness of this duality is new to biologists. In the words of virologist Stephen S. Morse of Columbia University, "The life sciences are losing their innocence."[3] At the same time, the vast potential of research on pathogens to enhance human welfare and yield countermeasures against bioterrorism rules out halting research and development in this field because of its potential for misuse.

Although improved disease surveillance and new vaccines and therapeutic drugs are clearly needed to combat bioterrorism, it is also essential to make it more difficult for terrorists or criminals to obtain deadly pathogens and toxins (poisonous chemicals made by living organisms). As Sandra Fry of the Canadian Food Inspection Agency has argued, in an age of international terrorism, the possession of biohazardous materials has become "a privilege, not a right."[4] The term "biosecurity" refers to policies and procedures designed to prevent the deliberate theft or diversion of deadly pathogens and toxins for malicious or criminal purposes. This report assesses the threat of pathogen diversion by terrorists

and criminals, reviews current U.S. and international efforts to strengthen biosecurity, and develops a framework for the negotiation of global standards.

Biosecurity vs. Biosafety

Although the terms "biosecurity" and "biosafety" are sometimes used interchangeably, they refer to different issues. Whereas biosecurity measures aim to prevent the *deliberate* diversion of deadly pathogens for malicious purposes, biosafety measures are intended to prevent *accidental* infections of researchers or releases of pathogens from a research facility that could endanger public health or the environment. Biosafety is achieved through various types of biocontainment, which involves placing impermeable barriers or filters between the infectious agent and the researcher, and between the laboratory and the environment. Types of biocontainment include good laboratory practice and technique, sealed glove boxes and biological safety cabinets, and specialized biocontainment laboratories equipped with air filters and fans that generate negative atmospheric pressure, so that a breach in containment causes air to flow into rather than out of the facility.

Four levels of biocontainment—referred to as Biosafety Levels (BSL) 1 through 4—provide increasingly stringent protection to personnel, the environment, and the community. Incurable disease agents such as hemorrhagic fever viruses must be studied in a maximum-containment (BSL-4) laboratory, whereas *Bacillus anthracis,* the causative agent of anthrax, can be handled in a BSL-2 or BSL-3 laboratory, depending on the nature of the experiment. Although anthrax is not contagious from person to person and can be treated with antibiotics, large quantities or high concentrations of anthrax spores, or aerosolization of the spores, push the required biocontainment level up to BSL-3.

The leading resource in the biosafety field is *Biosafety in Microbiological and Biomedical Laboratories,* published by the U.S. Centers for Disease Control and Prevention (CDC) and the National Institutes of Health (NIH).[5] Known by the abbreviation BMBL and now in its fourth edition, this manual is considered the "gold standard" for the safe conduct of laboratory research on dangerous pathogens. Since the BMBL was first published, there has been a marked decline in the number of accidental infections of laboratory workers and the escape of dangerous pathogens into the environment. The BMBL has also served as the model for biosafety guidelines issued by the World Health Organization (WHO). A separate set of safety guidelines for the licensed use of radioisotopes in research laboratories has also been widely accepted by scientists.

Gaps in Biosecurity

Until recently, the safeguarding of dangerous pathogens was viewed primarily as a matter of biosafety rather than biosecurity. But several publicized incidents of security lapses at U.S. government laboratories called attention to the need for stricter regulations in the United States and, by implication, in other countries as well. In May 2002, a report by the inspector-general of the Department of Agriculture found that many of the department's 124 research laboratories were vulnerable to theft, could not account accurately for stocks of animal and plant pathogens, and had granted numerous visiting scientists—including foreign nationals—unimpeded access to the laboratories.[6] Similarly, congressional and journalistic investigations of the Pentagon's leading biodefense facility, the U.S. Army

Medical Research Institute of Infectious Diseases (USAMRIID) at Fort Detrick, Maryland, uncovered chronic problems with laboratory security during the 1980s and 1990s, including repeated failures to account for missing samples of pathogens because of poor internal controls and recordkeeping. According to one whistleblower, no formal audits of the dangerous human pathogens stored at USAMRIID were ever conducted. When Army scientists were asked to account for hazardous materials, they simply photocopied an old inventory and changed the date.[7]

Unless the security lapses at U.S. government laboratories are corrected, recent increases in federal funding for research on defenses against bioterrorism could prove counterproductive. The 2003 federal budget provided a total of $1.7 billion in biodefense funding, including $1.497 billion for the National Institute of Arthritis and Infectious Diseases at the NIH, five times more than the year before.[8] About half of the NIH money ($746 million) is being devoted to the construction or expansion of high-containment laboratories and related infrastructure. Currently the United States has roughly twenty high- and maximum biocontainment (BSL-3 and BSL-4) laboratories, and plans or proposals exist to double that number through new construction and upgrades.[9] Additional federal BSL-4 laboratories are planned at Fort Detrick, the CDC, and Rocky Mountain Laboratory (an NIH facility in Hamilton, Montana).[10] In addition, two new BSL-4 and several BSL-3 research facilities will be housed at universities, which tend to be less secure than government labs.[11] Ironically, by greatly expanding the number of facilities and people working with pathogens, the boom in biodefense research could increase the risk of theft or diversion for malicious purposes unless biosecurity measures are improved significantly.[12]

Lack of International Standards

In 2002, Congress passed legislation to tighten controls over dangerous pathogens and toxins and reduce the risk that terrorists or criminals could acquire them from laboratory sources. Yet even as the U.S. government puts its own house in order, the international dimension remains problematic. No global standards for laboratory security currently exist on which individual states can base national legislation and regulatory structures. This lack of international harmonization has given rise to major gaps and vulnerabilities that must be addressed as part of a coordinated global strategy to prevent bioterrorism.

By helping to ensure that dangerous pathogens are used only for peaceful purposes, global biosecurity standards would reinforce the prohibition on the state-level development, production, and stockpiling of biological weapons enshrined in the 1972 Biological Weapons Convention (BWC).[13] Although this treaty has been ratified by some 150 countries, it lacks any formal system of monitoring and verification (unlike the 1993 Chemical Weapons Convention) and hence is little more than a gentleman's agreement. Efforts over the past two decades to put teeth in the BWC have been largely unsuccessful. At the regular five-year review conferences held in 1986 and 1991, member-states agreed to a number of politically binding confidence-building measures to bolster the treaty, such as filing annual reports on biodefense activities and unusual outbreaks of disease, but only a small minority of countries have complied.

More recently, a six-year effort to negotiate a legally binding protocol to strengthen the BWC through a system of mandatory declarations and on-site inspections of treaty-relevant facilities, along with investigations of alleged bioweapons use and suspicious outbreaks of disease, collapsed in July 2001 when the United States rejected the draft text. Bush administration officials argued that the proposed inspection system would not be effective at detecting treaty violations and posed an unacceptable risk of compromising sensitive biodefense information and commercial trade secrets belonging to the pharmaceutical and biotechnology industries.[14]

As an alternative to a multilateral agreement to strengthen the BWC, the Bush administration urged member-states to pass national legislation that would punish treaty violators and help to prevent bioterrorism. In November 2002, under U.S. pressure, the Fifth Review Conference of the BWC adopted a work program consisting of three annual meetings of experts groups and states parties in 2003–2005, prior to the next scheduled review conference in late 2006. The aim of the intersessional meetings is to "promote common understanding and effective action" on measures that could be taken at the national level to strengthen the BWC: penal legislation, pathogen security regulations, enhanced international procedures to investigate and mitigate the alleged use of biological weapons, improved mechanisms for global infectious disease surveillance and response, and scientific codes of conduct.[15] The first intersessional meeting of BWC member-states, held on November 10–14, 2003, addressed the enactment of national penal legislation and the development of best practices for security and oversight of pathogens and toxins.

In principle, it would be desirable to establish a set of legally binding standards for pathogen security in the form of an international treaty, or biosecurity convention, that includes provisions for international assistance and oversight.[16] Such a treaty would probably not impose significant additional constraints or burdens on the United States, but mainly on other countries. Nevertheless, negotiating a biosecurity convention could take years and, in any event, is not feasible in the current political environment given the Bush administration's strong aversion to multilateral arms control. For this reason, any short-term strategy for controlling access to dangerous pathogens will have to be based on international standards implemented through national legislation. At the same time, it is desirable to avoid institutionalizing policies and practices that would preclude a more comprehensive multilateral approach to strengthening the BWC when political circumstances become more favorable.

Two

The Threat of Pathogen Diversion

In order to design an effective international control system for dangerous pathogens, it is useful to analyze how terrorists would acquire them. With a few exceptions (such as the foot-and-mouth disease virus, which would not need to be weaponized), a biological weapon is not simply a sample of a pathogen or toxin, but rather a *system* consisting of (1) a quantity of agent—either in the form of a wet slurry or dry powder—that has been formulated with chemical stabilizers and other additives, (2) a container holding the hazardous material, and (3) a dispersal mechanism.

A small-scale biological attack designed to terrorize the public would entail far lower technical hurdles than one intended to inflict mass human casualties. Although the anthrax letter attacks involved a high-quality preparation of dried anthrax spores, the method of dissemination was rudimentary. Technologically novice terrorist groups might follow the published results of state biowarfare programs or improvise weapons from readily available materials; more sophisticated terrorists might recruit former weapons scientists or develop their own specialized expertise. It is also important to distinguish between *criminal* and *terrorist* use of biological agents. Whereas a biocriminal would probably wish to avoid attribution for an attack, a bioterrorist might well claim credit or, at the least, would want the authorities to recognize that a disease outbreak was deliberate rather than natural in origin.

The historical record suggests that bioterrorists are generally opportunistic and seek out the most accessible source of pathogens, much as a burglar tries doorknobs until he finds one that is unlocked. With the exception of the smallpox virus—an eradicated disease agent that is currently stored in only two official repositories in the United States and Russia—the roughly twenty-five infectious microorganisms considered suitable for bioterrorism could be obtained from natural sources, such as infected animals, patients, or even contaminated soil (in the case of anthrax spores). Nevertheless, because natural pathogens vary widely in virulence (that is, the degree to which a microorganism can cause disease), many strains isolated from nature may have low virulence. Microbiologists have catalogued more than seventy different strains of *Bacillus anthracis,* only a minority of which are highly virulent.[17] Thus, a terrorist would almost certainly have to isolate many different strains before finding one that was sufficiently potent to serve as a weapon.

Given the technical hurdles associated with obtaining virulent microorganisms from nature, it would probably be easier for terrorists to steal well-characterized strains from a research laboratory. The Ames and Vollum strains of anthrax, for example, are known to be highly virulent. Bioterrorists might also seek to purchase known pathogenic strains from a national culture collection or a commercial supplier under false pretenses by claiming to be engaged in legitimate biomedical research. Between 1985 and 1989, for example, the government of Iraq ordered virulent strains of anthrax and other lethal patho-

gens from culture collections in France and the United States, ostensibly for public health research—a purpose for which U.S. exports to Iraq at that time were legal and indeed approved by the Department of Commerce. Nevertheless, the imported agents soon found their way into the Iraqi biological warfare program.[18]

Enhanced biosecurity is not a panacea for the problem of bioterrorism. Since a skilled microbiologist could isolate pathogens and toxins from natural sources, the goal of biosecurity measures is to make terrorist acquisition of deadly agents more difficult, albeit not impossible, by ensuring that legitimate research activities and facilities remain off-limits. In that case, determined bioterrorists would be forced to obtain dangerous pathogens from natural sources, a route that demands greater technical skill and is considerably less reliable.

Nuclear Safeguards: How Relevant?

The National Commission on Terrorism, chaired by L. Paul Bremer III, recommended in June 2000 that "standards for the storage, transport, and handling of biological pathogens should be as rigorous as the current standards for the physical protection of critical nuclear materials."[19] Yet, how relevant are nuclear safeguards to biosecurity?

Because the two fissile materials used in nuclear explosive devices, plutonium and highly enriched uranium (HEU), do not exist in nature and are extremely difficult and costly to produce, terrorist organizations seeking to build nuclear weapons would have to steal or otherwise divert fissile materials from an existing production or storage facility. Thus, from the dawn of the nuclear age, U.S. government officials established strict security rules for fissile materials, including physical barriers and access controls at defense nuclear facilities, quantitative tracking of inventories of weapons-grade material, and personnel reliability programs. After the entry into force of the 1968 Treaty on the Nonproliferation of Nuclear Weapons, the International Atomic Energy Agency (IAEA) negotiated safeguards agreements with member countries that operate civilian nuclear power reactors, which can generate plutonium as a byproduct of energy production.

The task of securing and controlling fissile materials is facilitated by some inherent characteristics of HEU and plutonium: they are detectable at a distance by their radioactive emissions, can be inventoried and tracked fairly reliably, and would have to be stolen in kilogram quantities to be usable for weapons purposes.[20] Nuclear safeguards comprise two complementary approaches: physical protection, and materials control and accounting. Physical protection includes barriers, surveillance systems, alarms, guards, portal monitors that sound an alarm if someone attempts to remove radioactive material, and procedural approaches such as the two-person rule, by which all staff members must be accompanied to enter or work in a secure area. Materials control and accounting (MC&A) systems involve the use of precise measuring equipment and computerized accounting systems to track the amounts and locations of fissile materials in a nuclear facility. The goal is to maintain a "mass balance" between the quantity of material entering the plant and that remaining inside, leaving the site, or lost to waste. Any significant discrepancy between inputs and outputs could indicate the deliberate diversion of fissile material.[21]

In contrast to nuclear safeguards, measures to prevent the deliberate misuse of biological pathogens have historically been weak. Collections of dangerous pathogens and toxins have been stored in unsecured freezers and shipped across national borders with minimal

security precautions. University-based researchers have a long tradition of sharing microbial cultures informally through the mail, and few countries regulate who is granted access to pathogens. In part, this laxity arose from the fact that in the pre-September 11 environment, biological threats were not recognized to be as dangerous as nuclear ones. Major differences between biological and nuclear materials also affect the relevance and effectiveness of certain types of controls. Characteristics of pathogens that limit the applicability of the nuclear safeguards model include the following:

1. **Pathogens occur naturally.** Whereas HEU and plutonium are synthetic materials that do not exist in nature and are difficult and costly to produce, most biological pathogens (with the exception of the smallpox virus) can be obtained from natural sources, such as diseased animals or even soil. Thus, bioterrorists would not have to rely exclusively on stealing pathogens from a research laboratory or culture collection, although obtaining a known, well-characterized strain from such a source would increase their confidence in the desired properties.

2. **Pathogens are dual-use.** Many pathogens that could be stolen or diverted for malicious ends have legitimate applications in biomedical research or for the development, production, and testing of vaccines, drugs, and diagnostic tools. The equipment used to cultivate and process pathogens is also dual-use. Although weapons-grade fissile materials have a few nonmilitary applications in research reactors, thermoelectric generators, and the production of radioisotopes, these applications are more specialized and less widely distributed than civilian uses of pathogens.

3. **Pathogens are highly diverse.** Whereas plutonium and HEU are the only fissile materials used to make nuclear weapons, a variety of pathogens are suitable for bioterrorist attacks. For example, the Rajneeshee cult in Oregon used *Salmonella* —a nontraditional biowarfare agent—to contaminate restaurant salad bars. Benign microorganisms might also be rendered pathogenic through genetic engineering techniques, such as the insertion of toxin genes.

4. **Pathogens can reproduce.** Unlike fissile materials, infectious microorganisms reproduce rapidly under the right conditions, so that a small "seed culture" of anthrax bacteria could be cultivated under optimal growth conditions to yield a large quantity of agent in a matter of days. For this reason, the theft of even minute quantities of a pathogen can pose a security threat. Moreover, the materials-balance approach, in which a hazardous material is tracked quantitatively as it enters, passes through, and exits a facility, is not feasible with self-replicating biological agents.

5. **Pathogens are not detectable at a distance.** Fissile materials give off ionizing radiation that can be picked up by sensitive instruments up to several feet away, making it possible to detect nuclear smuggling at a facility exit or a border crossing. In contrast, biological pathogens and toxins have no comparable signatures that can be detected at a distance with currently available technologies. A terrorist could smug-

gle freeze-dried pathogens in sealed plastic vials through a security checkpoint with little risk of detection.

6. **Pathogens are present in many types of facilities.** Whereas weapons-grade fissile materials are restricted to roughly a hundred nuclear sites worldwide, dangerous pathogens and toxins are stored and manipulated in thousands of facilities, including hospitals, universities, clinical laboratories, biotechnology firms, and state and federal laboratories.[22] A terrorist organization wishing to steal pathogens would probably target a particular facility either because it had lax security or housed a highly virulent strain that was not available elsewhere.

7. **Pathogens can be present at multiple locations within a facility.** Whereas fissile materials tend to be consolidated inside a facility, infectious agents may be dispersed in several locations, including storage freezers, laboratory incubators, living experimental animals, animal carcasses, and waste materials. For these reasons, the total inventory of a pathogen being utilized in a research lab cannot be determined precisely at any given time. Accounting of biological pathogens is particularly difficult when they are being subcultured and used for experimentation.

8. **Pathogens can be derived from benign microbes or even made "from scratch."** With advances in genetic engineering, it has become possible in principle to convert a harmless microbe into a pathogenic one. In early 2001, Australian researchers reported that inserting a single gene for an immune-system protein into the mousepox virus rendered it highly lethal and vaccine-resistant in mice.[23] Similar manipulations may be effective in poxviruses that infect humans, such as smallpox, vaccinia, or monkeypox. Scientists have also built a pathogenic virus in the test tube. In July 2002, researchers at the State University of New York at Stony Brook announced that they assembled short segments of synthetic poliovirus DNA (ordered from a scientific supplier based on the published DNA sequence) into the complete viral genome, which began to replicate spontaneously.[24] Although poliovirus has an extremely small genome (7,741 DNA base pairs), advances in technology may make it possible to synthesize more complex viruses such as Ebola, whose genome is about two and one-half times larger. It will probably be several years, if ever, before scientists can synthesize viruses as complex as smallpox, which has nearly 200,000 DNA base pairs. Nevertheless, it may be feasible to modify the DNA sequence of a closely related poxvirus, such as vaccinia or camelpox, to render it more virulent.

The fact that microbial pathogens exist naturally in the environment and that small samples can be grown into large quantities means that biological materials cannot be controlled as effectively, or in the same manner, as fissile materials. Since no technology or procedure can ensure the quantitative accounting of pathogens, applying controls based on nuclear safeguards to biological laboratories would create a false sense of security while seriously impeding legitimate research. It is therefore essential to develop a new security paradigm tailored to the unique characteristics of microorganisms and the vulnerabilities of the facilities that work with them.[25]

Three

U.S. Biosecurity Legislation

The United States introduced controls on dangerous pathogens in the mid-1990s after a troubling incident called the attention of policymakers to the lack of federal regulations in this area. In February 1995, Larry Wayne Harris, a licensed microbiologist in Columbus, Ohio, ordered three vials of freeze-dried *Yersinia pestis* (the bacterium that causes plague) from American Type Culture Collection (ATCC), a private, nonprofit corporation near Washington, D.C. that supplies microbial cultures to biomedical researchers.[26] Harris was employed by a commercial laboratory in Columbus, where he tested samples of drinking water and inspected septic systems. In his free time, however, he was a neo-Nazi sympathizer who was writing a survivalist manual on how to defend against biological warfare. Although no law prohibited Harris from purchasing cultures of dangerous pathogens through the mail, he misrepresented himself by placing his order on forged letterhead that purported to be from a commercial laboratory. After Harris's repeated calls to ATCC to check on his order aroused suspicion, the police confiscated the plague cultures. He was arrested and subsequently convicted of one count of mail fraud.[27]

In response to the Harris case, Congress incorporated into the Anti-Terrorism and Effective Death Penalty Act of 1996 (Public Law 104-132) a section requiring the Department of Health and Human Services to regulate transfers of dangerous human pathogens and toxins to prevent their acquisition by terrorists and criminals. According to federal regulations effective April 15, 1997, anyone shipping or receiving one or more of the twenty-four infectious microbes and twelve toxins that federal officials had designated as possible bioterrorism agents had to register with the CDC and declare a legitimate scientific or medical use for the material. Both the shipper and the recipient were also required to report each transfer of a "select agent" to a central registry. Violations of the registration and transfer rules were punishable by prison terms and fines of up to $500,000. Under the 1997 regulations, 335 facilities involved in transfers of select agents registered with the CDC.[28]

In part because of resistance from the scientific community, however, the regulations contained a major loophole. Laboratories that possessed or worked with select agents obtained before the regulations entered into force, and that did not transfer or receive them after the effective date, were not required to register. In an attempt to close this loophole, Senators John Kyl (R-AZ) and Diane Feinstein (D-CA) co-sponsored a bill called the Counterterrorism Act of 2000 (S.3205), which expanded the select agent rules to cover possession. Although the bill passed the Senate during the 106th Congress, the House of Representatives did not have time to consider it.

Several months later, the terrorist attacks of September 11, 2001, and the ensuing anthrax-tainted letters transformed official perceptions of the bioterrorism threat and led

to a flurry of new legislation. On October 26, 2001, President George W. Bush signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act. Section 817 of this act makes it a crime for a person knowingly to possess any biological agent, toxin, or delivery system that cannot be "reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose." Violations are punishable with a $10,000 fine, ten years' imprisonment, or both. In addition, Section 175b specifies several categories of *restricted persons* who are prohibited from shipping, receiving, transporting, or possessing select agents:

- Aliens, other than permanent residents, from countries on the State Department's list of states that support international terrorism.[29]
- Persons who admit using or are convicted users of a controlled substance.
- People under indictment or convicted of a crime punishable by imprisonment for more than one year.
- Veterans dishonorably discharged from the U.S. armed services.
- Fugitives from justice.
- Aliens illegally in the United States.
- Persons judged to be "mentally defective" or committed to a mental institution.

One problem with the restricted-persons provision of the USA PATRIOT Act is that some of the exclusion criteria are not available on government databases, such as whether an individual has engaged in unlawful use of controlled substances without being convicted or is a "mental defective." State privacy laws and university policies may also prevent inquiries into the mental health records of students or staff members. Furthermore, the USA PATRIOT Act lacks an appeal mechanism for those who are automatically excluded by its provisions. According to critics, the blanket application of the restricted-persons rule could harm the atmosphere of scientific openness that has made the United States a world leader in bioscience research.[30]

Bioterrorism Preparedness Act

During Senate Judiciary Committee hearings after the fall 2001 anthrax letter attacks, officials from the Federal Bureau of Investigation (FBI) testified that because of the loophole in the 1997 select agent regulations, the U.S. government did not have a comprehensive list of facilities and scientists in the United States that possessed or worked with anthrax, hampering the FBI's ability to identify the perpetrator(s) of the letter attacks. This realization led Congress to include a section on "Enhancing Controls on Dangerous Biological Agents and Toxins" in the Public Health Security and Bioterrorism Preparedness and Response Act, which President Bush signed into law on June 12, 2002.

All facilities and persons in the United States that possess, use, or transfer listed human pathogens and toxins, or listed plant and animal pathogens, must register with the CDC or the U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS), respectively. ("Overlap" agents that affect both human and animal health may be reported to either agency.) In addition to pathogens and toxins, the select agent list includes genetic elements, recombinant microorganisms, and DNA strands that encode a listed virus or toxin in a form capable of replication. Excluded from the reporting requirement are dead or inactivated microorganisms and certain "attenuated" (weakened) strains. To avoid hampering medical diagnostic practice, the law exempts clinical laboratories that isolate select agents from human specimens, record the results, and destroy the cultures within one week; however, clinical laboratories that preserve reference specimens of select agents must register. The CDC and APHIS are required to review and republish the select agent lists every two years, taking account of scientific and technical advances and making modifications as needed to protect the public. (For the current list, see the appendix.)

According to the Bioterrorism Preparedness Act, all facilities that possess listed agents must conduct an inventory of the pathogens and toxins in their possession, eliminate those for which they have no legitimate need, and keep track of who is working with listed agents and the locations where they are used.[31] Registered facilities must implement safeguard and security measures to prevent terrorists from gaining access to the agents in their possession. In addition, the Act requires background checks, or "security risk assessments," of scientific personnel who wish to work with listed agents.[32] Registered laboratories must send a list of names to the Department of Justice, and applicants are required to fill out a web-based application form and submit fingerprints. This information is forwarded to the FBI for screening against criminal, immigration, terrorism, and national security databases. If an applicant is not cleared, an appeal is possible unless the individual falls into one of the categories of restricted persons listed in the USA PATRIOT Act. Because the clearance process is facility-based, however, scientists may need to undergo another background check if they move to a different laboratory.

The new regulations took effect on February 12, 2003, with a highly compressed timetable for implementation, and violations are subject to criminal penalties.[33] A research team at Sandia National Laboratories has estimated that a total of 1,167 entities possess select or overlap agents or toxins in nonagricultural use. Of these, 350 laboratories perform only diagnostic work and are therefore excluded, leaving 817 entities that must register with the CDC under the select agent rule. An additional 33 entities possess listed plant pathogens, and 619 possess listed animal and overlap pathogens and toxins in agricultural use—a total of 652 entities that must register with APHIS. Thus, an estimated total of 1,469 facilities will be affected by the new U.S. biosecurity regulations. (The figure may be somewhat lower if USDA and HHS are double-counting facilities that work with overlap agents.[34])

Laboratory Security Measures

The main purpose of the U.S. biosecurity regulations is to determine who, what, and where—to keep close track of who has access to select agents, what agents have been accessed, and where in a facility they are in use. Each institution that declares listed patho-

gens and toxins must conduct threat, vulnerability, and risk assessments, followed by the development of a comprehensive security plan to protect areas containing the listed agents. Because of the wide range of entities that work with select agents, security measures must be tailored to the characteristics of each facility, including its location and principal function, the types and quantities of select agents stored on-site, and the assessed risk to the health of humans, livestock, or crops.[35] Once an institutional security plan has been developed, it is submitted to the CDC or APHIS, performance-tested, and updated periodically. Federal inspectors are empowered to visit registered facilities at any time, unannounced, to conduct on-site inspections and examine records.

Some critics note that the new biosecurity rules permit considerable leeway in interpretation, running the risk that similar facilities will implement different levels of protection.[36] In December 2002, the CDC issued a revised and expanded set of security guidelines (formerly appended to the BMBL) titled "Laboratory Security and Emergency Response Guidance for Laboratories Working with Select Agents."[37] Although this document is helpful, it is still rather vague. Academic institutions developing laboratory security plans will require more detailed guidance, probably in the form of a handbook that is the biosecurity equivalent of the BMBL. The U.S. Department of Agriculture, for example, has contracted with Sandia National Laboratories for the preparation of a "Reference Manual for Biosecurity."[38] Until such resources become available, professional societies such as the American Society for Microbiology (ASM) and the American Biological Safety Association (ABSA) are attempting to fill the gap by providing information and holding conferences for scientists and administrators on how to implement the new regulations.

Since the tightened rules went into effect, primary investigators working with select agents have been required to spend a great deal of time documenting compliance. The resulting paperwork burden and costs, as well as concerns over legal liability and loss of privacy, could create disincentives for research on dangerous pathogens at a time when the U.S. government is pushing for an increase in biodefense activities. Even more worrisome, the regulations may lead some laboratories to destroy rare archival stocks of human, plant, or animal pathogens needed for the forensic identification of agents used in bioterrorist attacks and the development of defenses. Anecdotal data suggest that the tightened biosecurity regulations have already had a chilling effect on U.S. academic research. At Duke University, fifty-seven laboratories were working with select agents before the regulations went into effect; within a few months, six of the labs discontinued work with select agents, one destroyed its stocks, and two transferred them.[39]

Another problem is that the new regulations impose an undue financial burden on academic researchers, especially those working in smaller laboratories.[40] Fearing legal problems, some academic institutions have required laboratories working with select agents to hire a full-time biosecurity officer to ensure compliance with the new regulations. At present, there is a 26 percent cap on indirect costs associated with regulatory compliance that recipients of federal grants can charge to the U.S. government. To avoid driving academic institutions away from biodefense research, the government may have to cover a larger percentage of regulatory overhead.

Four

The International Dimension

Even as the United States implements tightened biosecurity regulations, the international dimension of the problem remains to be addressed. Many countries conduct research on infectious disease agents and maintain collections of dangerous pathogens. The anthrax bacterium, for example, is studied widely because it poses an endemic threat to animal and human health in many parts of the world. In addition, more than a dozen countries operate maximum-containment (BSL-4) laboratories designed for work with the most deadly and incurable pathogens.[41] Because scientific research on dangerous pathogens is international, any campaign to restrict terrorist access to biohazardous materials must also be global in scope.

One area of particular concern is the legacy of past offensive biological warfare programs. At the apogee of the Soviet program during the late 1980s, some 60,000 scientists and technicians participated in bioweapons research and development at dozens of institutes and production facilities scattered across the USSR.[42] Today, many former bioweapons-related facilities—now in the Soviet successor states of Russia and Kazakhstan—have been converted to civilian activities. Nevertheless, they continue to possess collections of highly dangerous pathogens that potentially could be stolen or diverted for military, terrorist, or criminal purposes.

During the Soviet era, institutes involved in biowarfare research had well-developed accounting and control systems for the dangerous pathogens they worked with. Employees were required to record in special logbooks every test tube, petri dish, or flask containing a bacterial or viral culture, even those intended for destruction, and scientists and technicians were not allowed to work in laboratories alone. In the context of a totalitarian system, these security measures created an environment in which it was difficult for workers to steal or divert dangerous strains.[43] After the breakup of the Soviet Union, however, the old structures of authority and control collapsed, along with the economic safety net. Accordingly, pathogen collections in the former Soviet states are now at risk of outsider theft and insider diversion. Although improved biosecurity measures are urgently needed, many laboratories—such as those associated with the former Soviet network of Anti-Plague Institutes and field stations—lack the financial and technical resources to implement them.

A recent incident suggests that the risk of pathogen theft is real. In November 2002, authorities in Almaty, Kazakhstan, arrested a man who entered the Scientific Center of Quarantine and Zoonotic Infections, a laboratory specializing in research on veterinary and plant diseases, at the end of the work day with the apparent intent of stealing pathogens. Fortunately, the intruder was arrested before he could get past the second layer of physical security, which had recently been upgraded with U.S. government assistance.[44] Equally worrisome is the potential diversion of pathogens by scientists and technicians

working at the former biowarfare institutes. Deprived of the high salaries and perks they enjoyed during the Soviet era, these individuals could be tempted to divert small quantities of weaponized pathogens and sell them to foreign agents or terrorists seeking a biowarfare capability.

Another former bioweapons program whose legacy poses an ongoing proliferation threat was that conducted by South Africa from 1981 to 1993. Known as Project Coast, this program did not yield militarily significant quantities of biowarfare agents but focused instead on developing small-scale, custom-made weapons to terrorize or kill opponents of the apartheid regime. Project Coast scientists collected hundreds of strains of deadly pathogens, including forty-five types of anthrax bacteria and cultures of the agents that cause cholera, brucellosis, and plague. Although South African officials claimed that all of the pathogens were destroyed when the program was dismantled in 1993, this assertion was never verified and has recently been called into question. According to the *Washington Post,* former Project Coast scientists "retained copies of bacterial strains to continue work on vaccines and antidotes with commercial applications" and tried to sell some of the strains to the United States government and possibly to other countries. Today the fate of several deadly pathogens studied by South Africa, including genetically engineered strains, remains unknown.[45]

Security risks are also associated with about one-third of the roughly fifteen hundred state-owned and commercial culture collections worldwide that possess, exchange, and sell samples of microorganisms and toxins for legitimate scientific and biomedical research.[46] Culture collections vary widely in size and content, ranging from large organizations such as ATCC and the U.S. Department of Agriculture's library of plant and animal pathogens in Ames, Iowa, to small "boutique" collections of microbial strains at universities, federal agencies, and private companies. Many culture collections outside the United States are not adequately secured and controlled, making them potentially vulnerable to theft by proliferators and terrorists. Trade in microbial cultures is also poorly regulated, both within countries and among them. Because international terrorist organizations are likely to seek biowarfare materials from the most accessible sources, the continued availability of dangerous pathogens from commercial suppliers poses a threat to international security.

France, Germany, Israel, Japan, and Great Britain, in addition to the United States, have passed domestic legislation relating to laboratory security.[47] On June 13, 2003, the Council of the European Union (EU) issued an action plan for countering the proliferation of weapons of mass destruction. Item 18 of this plan calls on EU members to develop best-practices guidelines to promote the enactment of national legislation for controlling dangerous pathogens and toxins.[48] To be effective, however, national regulations must be both comprehensive and reasonably uniform. Relying exclusively on nonharmonized national legislation would result in a patchwork of inconsistent regulations, including pockets of weak implementation or enforcement that terrorists could exploit to target poorly protected facilities.

Only the promulgation of global biosecurity standards would address this problem. Harmonized standards would also facilitate international collaborative research on biodefense vaccines and drugs. For example, incompatible national regulations on transfers

of dangerous pathogens have impeded joint U.S.-Russian research projects on defenses against anthrax and smallpox.[49] Because the United States is already implementing stringent biosecurity regulations, the burden of negotiated global standards would fall primarily on those countries that currently fail to ensure even minimal levels of pathogen security.

International Biosecurity Initiatives

One possible approach to the development of global biosecurity standards would be to start at a regional level or with a group of like-minded states and then expand to a more inclusive regime. Recently, several international organizations have launched partial initiatives in this area.

World Federation for Culture Collections

The World Federation for Culture Collections (WFCC) is a loose association that promotes the preservation of microorganisms and other biological resources. At the federation's annual meeting in 2001, American Type Culture Collection proposed creating a mechanism to harmonize security standards among the members, but this proposal did not gain much support.[50] Instead, the federation issued the following policy statement: "The WFCC urges its members to strictly follow all national and international legislations concerning distribution of sensitive materials to third parties."[51] The U.S. Federation for Culture Collections and the European Culture Collections Organization have issued similar statements.[52] Unfortunately, these organizations lack the authority to monitor and enforce compliance. Even if the policy statements could be enforced, they do not establish a minimum biosecurity standard worldwide and hence do not prevent weak standards in some nations from undercutting more stringent standards in others.

Organization for Economic Cooperation and Development

To date, the most ambitious international effort to secure dangerous pathogens has been launched by the Organization for Economic Cooperation and Development (OECD), a group of thirty-one advanced industrial countries (including the EU as one member) headquartered in Paris. The OECD has long been interested in "biological resource centers" (BRCs), defined as government, industry, or academic facilities that house, control, test, and use biological resources such as microorganisms, cell lines, DNA, and tissue samples.[53] BRCs are a key element of the research infrastructure for the life sciences and biotechnology.[54] The OECD initiative aims to establish a global network of BRCs to ensure the availability of rare biological resources as private culture collections disappear and governments withdraw financial support. The planned BRC network would permit the free exchange of microbial cultures among its members, functioning as a virtual lending library to encourage curation, research, and stable funding.

In mid-2001, the OECD established a Task Force on BRCs to begin negotiations toward the establishment of the global network, including the harmonization of national standards and regulations. To this end, the Task Force is negotiating a set of standards for participation in the network that will be presented for approval at a meeting of science ministers from participating countries scheduled for the last week of January 2004. The

most active members of the BRC Task Force are the United States, the United Kingdom, Ireland, France, and Japan. In addition to regular members of the OECD, about a dozen nonmember countries have been invited to participate as observers, including Brazil, Burkina Faso, China, Israel, Laos, Malaysia, Philippines, Russia, Senegal, South Africa, Thailand, and Vietnam.

Initially the OECD talks focused on criteria for the certification of BRCs, including quality-control and quality-assurance standards for the composition and purity of cultures. After the terrorist attacks of September 11, 2001, the United States requested that the mandate of the BRC Task Force be expanded to include biosecurity.[55] The Task Force's overall approach is similar to that of the U.S. regulations, including the requirement to keep pathogens under lock and key and to grant access only to scientists who have a legitimate need for the materials and have been appropriately vetted. To certify and enforce the agreed standards on a national basis, the OECD Task Force will set up an accreditation system. Each participating government will select a certifying agency, which will conduct periodic checks of biosafety and biosecurity at the participating BRCs. The certifying body may be an academic or nongovernmental organization, domestic or foreign. Francophone African countries, for example, may prefer a French agency.

Given the deadline for ministerial sign-off in January 2004, the BRC standards will probably be fairly modest and general, and will not be legally binding.[56] Nevertheless, because the exchange of pathogens within the BRC network will require all participating facilities to be reasonably secure, those countries that do not meet the standards will be excluded from participation. "The system will work on the basis of carrots rather than sticks," says OECD staff scientist Iaian Gillespie. "Participation will be based on a voluntary agreement, but with the condition of meeting some minimum standards."[57]

OECD members are conducting regional consultations with nonmember states, with a view to creating a global network of BRCs. Eventually the network could be spun off from the OECD, with the possible creation of a small international secretariat to serve as gatekeeper. Because the goal of the BRC network is to maintain high-quality cultures and to build capacity over time, it may be necessary to develop a tiered system. According to Gillespie, "Developing countries might get in at the first tier and rise up through a stepped series of quality standards. One could apply the same philosophy to the security dimension." [58] Although compliance with a set of minimum biosecurity standards might be required for participation in the network, member-states would be expected to adopt tougher standards as they become more technically proficient.

Global Health Security Action Group

In response to the anthrax letter attacks in fall 2001, the health ministers of the Group of Seven (G-7) countries—Canada, Japan, France, United Kingdom, Germany, Italy, and the United States—plus Mexico met in Ottawa on November 7, 2001, and committed themselves to a new partnership called the Global Health Security Action Group. Among the group's stated objectives is to "to improve linkages among laboratories, including Level Four laboratories, in those countries which have them."[59] In 2002, the directors of BSL-4 laboratories in G-7 countries (plus Russia and Sweden) met in Lyons, France, to discuss how to improve communication among their facilities. A subsequent meeting established

an International High Security Laboratory Action Network to develop diagnostic tests and materials and avoid wasteful duplication of effort.[60] The BSL-4 network plans to develop standard biosecurity protocols for the transfer of pathogens from one laboratory to another.[61]

Australia Group

The United States and 32 other like-minded nations harmonize their national export controls on dual-use chemical and biological materials and equipment through an informal coordinating mechanism known as the Australia Group (AG). This body was established in 1985 following the widespread use of chemical weapons by Iraq during the Iran-Iraq War.[62] In 1990, in response to growing concerns about biological weapons proliferation, AG members agreed to tighten national export controls on a list of dangerous pathogens and dual-use biotechnology production equipment. On June 5, 2003, fourteen human pathogens were added to the Biological Control List.[63] Although historically the AG has aimed at preventing state-level proliferation, the group recently decided to place greater emphasis on the bioterrorist threat.[64] According to one official, the changes to the list reflect the fact that "a terrorist doesn't need to get the worst of the worst. All you need is something pretty bad and you cause a lot of harm and a lot of panic."[65] A major limitation of the AG, however, is that several important exporters of pathogens are not members.

Other International Initiatives

A few other international organizations have taken preliminary steps to enhance biosecurity measures. The Organization for Security and Cooperation in Europe has proposed standards for licensing and enforcement procedures related to dangerous pathogens and dual-use biotechnology equipment. The World Customs Organization has begun information-sharing with the International Criminal Police Organization (ICPO-Interpol) and the World Health Organization to combat the smuggling of biological, chemical, and radioactive materials. The International Maritime Organization plans to negotiate agreements to halt the shipping of biological agents for hostile purposes and to criminalize the use of biological weapons on maritime vessels.[66]

Pharmaceutical trade associations have also called for efforts to enhance biosecurity. In 2002, Interpharma, which represents the Swiss companies Novartis, Roche, and Serono, developed a draft code of conduct, "Biosafety and Biosecurity – Industry Best Practices to Prevent Use of Biohazardous Material." This document calls for the establishment of company-internal regulations and procedures, including detailed inventories of biological materials stored and transferred, transparency in the acquisition of dangerous pathogens and toxins from commercial sources and scientific collaborators, safe and secure transport of biological materials, treatment of wastes to avoid the discharge of infectious materials into the environment, and security measures to prevent access to pathogens by unauthorized individuals.[67]

Five

Global Biosecurity Standards

Because facilities that house and work with dangerous pathogens and toxins range from pharmaceutical companies to academic research laboratories, specific biosecurity measures cannot be developed on a "one size fits all" basis. Moreover, whereas advanced industrialized countries can implement biosecurity standards with capital-intensive measures such as electronic access controls, developing countries may need to rely on more labor-intensive means such as armed guards. For these reasons, guidelines for laboratory security should consist of functional requirements that the affected entities can implement in a tailored manner.[68]

Since it is not possible to protect all assets against every conceivable threat, it is essential to prioritize risks, balancing the complexity and cost of security measures against the threats posed by the pathogens held or used at a particular facility. Laboratories face two main types of diversion threats—from outsiders and insiders. The outsider threat consists of criminals or terrorist cells who attempt to break into a research facility, as well as visiting scientists, students, or short-term contractors who steal or divert pathogens during a visit or stay at the facility.[69] The insider threat, in contrast, involves trusted members of the scientific or technical staff who have been granted unescorted access to pathogens and are familiar with laboratory security procedures and equipment. Such individuals might be motivated to divert pathogens for several possible reasons: resentment over perceived unfair treatment, such as being reprimanded or passed over for promotion; financial pressures; blackmail threats; psychological or personal problems, such as divorce or substance abuse; and recruitment by a terrorist organization.

Biosecurity measures should be tailored to both outsider- and insider-type scenarios. Traditional approaches to facility security, often referred to as "guns, gates, and guards," can prevent unauthorized outsiders from penetrating a facility with the intent of stealing pathogens; however, such methods cannot stop a trusted staff member from diverting a small sample of pathogen for illicit purposes. For this reason, biosecurity should involve an integrated approach that combines physical protection, access control, materials management, and personnel screening. In addition to an emergency response plan in case of biosecurity breaches, the global standards should include, at a minimum: (1) mechanisms to account for pathogens that are being stored, used during experiments, or transferred or exported; (2) the registration and licensing of facilities that work with dangerous pathogens; (3) physical security at these facilities; and (4) procedures for screening laboratory personnel. These *preventive* elements are discussed in greater detail below.

Accounting Mechanisms

List of Pathogens and Toxins

To serve as a basis for biosecurity standards, it may be useful to develop a list of microbial and toxin agents of bioterrorism concern, with the CDC and APHIS lists providing a possible model. Skeptics argue that any select-agent list would become rapidly obsolete, and that countries have different priorities about which disease agents warrant protection. According to Professor D. Jay Grimes, a U.S. microbiologist, "Nations are unlikely to agree on a single list. But we may end up with a system in which each country recognizes and respects the lists of other countries."[70] If the participating states do decide to develop a common select-agent list, it would be useful to categorize pathogens and toxins according to level of threat, with the most dangerous agents warranting higher levels of physical protection and access control.

The CDC has grouped bioterrorist threat agents into three categories (A, B, and C) based on their impact on public health, with the top category comprising the microbes that cause smallpox, anthrax, plague, botulism, tularemia, and viral hemorrhagic fevers.[71] Alternatively, Reynolds Salerno and his colleagues at Sandia National Laboratories have proposed that the federal government rank pathogens and toxins along two dimensions: public health impact (for example, infectivity, pathogenicity, lethality, and transmissibility) and suitability for use as a bioterrorist weapon (for example, availability, ease of production, ease of processing to facilitate dispersal, environmental hardiness, availability of prophylactic or therapeutic countermeasures, and ability to mimic a natural disease outbreak).[72] Using the latter criteria, it would be reasonable to include pathogens that cause food- and water-borne diseases. Although some prioritization of agents according to risk is essential, it is also important to recognize that any attempt to establish a cutoff level of hazard for the imposition of biosecurity measures could invite terrorists to select pathogens just below the specified threshold.[73]

When developing a select list of pathogens and toxins as the basis for a regulatory regime, several questions need to be addressed. Should the list be broadly inclusive or limited to the most dangerous pathogens? Should it include lethal strains that kill slowly, such as multiple-drug resistant tuberculosis? Should the list specify agents at the level of strains, substrains, or unique identifiers (for example, DNA markers) to permit forensic analysis and tracing? Should it include virulence factors and toxin genes that might be transferred by genetic engineering to transform a benign microbe into a pathogenic strain or to enhance the virulence of an existing pathogen?

Rapid change in the field of biotechnology has also complicated the task of preparing a list of select agents. The test-tube synthesis of poliovirus in 2002, for example, raised the issue of whether synthetic DNA should be regulated. In the United States, roughly a half-dozen companies manufacture short strands of DNA called oligonucleotides to order, and several major universities have an in-house capability to produce them. An oligonucleotide can range from a few DNA units to more than two hundred; the shorter strands generally lack distinctive sequences that could identify them as part of a dangerous pathogen. For this reason, terrorists seeking to create a pathogenic virus might order

several seemingly benign pieces of DNA from different suppliers and then assemble them into a lethal agent. Alternatively, technically sophisticated terrorists might purchase a used DNA synthesizer and produce the oligonucleotides themselves.[74] Given the major technical hurdles involved in the test-tube synthesis of large viruses such as smallpox, however, the availability of custom-made DNA is unlikely to pose a major threat for the foreseeable future.

Inventory controls

Facilities working with select agents should establish procedures for pathogen accountability, including requirements for sample labeling, tracking of internal possession and transfers, and inactivation and disposal of cultures after use. Such inventory controls provide important administrative benefits by keeping track of which pathogens are stored at the facility, their locations, and who is responsible for them at any given time. Yet a pathogen accountability system is not a foolproof means of detecting or deterring the theft of material by a trusted insider. Because microorganisms are self-replicating, a scientist who has access to a pathogen could covertly remove a small sample of agent from the working stock and later grow it in large quantities. Nevertheless, recent U.S. government inspections of laboratories working with select agents have focused largely on inventory controls, including maps that show the freezer locations of vials containing pathogen cultures.

Is there a proven technical approach for detecting the diversion of pathogens from the laboratory? The investigation of the anthrax-tainted letters highlighted the importance of "microbial forensics"—the use of advanced molecular techniques to determine the strain of a microorganism and its geographical source in an effort to identify the perpetrators of a bioterrorist attack. Each time a pathogen is subcultured, random genetic mutations may be introduced that are unique to that particular strain. Thus, the particular strains housed at a given laboratory could be identified by small differences in their DNA sequence by means of a technique known as "genetic fingerprinting." In addition, radioisotope ratios (that is, the naturally occurring presence of rare isotopes, such as carbon 13, nitrogen 15, or oxygen 18) can help to determine the age and geographical origin of a culture, and other biochemical markers may provide useful identifiers.[75] At present, however, laboratories that possess select agents are not expected to profile them with genetic fingerprinting or other techniques. Requiring registered laboratories to record unique strain identifiers would make it easier to trace the source of a pathogen that has been stolen and used in a bioterrorist attack.

Another approach to tracking pathogens would be to "brand" particularly dangerous strains with an inserted DNA marker sequence that is unique to the originating laboratory. Such labeling would be analogous to the use of chemical taggants to identify the manufacturer of explosives used in terrorist bombings. Unfortunately, this idea is probably unworkable for a number of reasons. An inserted DNA marker sequence could be used only to identify new cultures, not archived stocks. Even if the DNA insert is "silent," meaning that it does not code for any genetic traits, it could render the microbial genome unstable, resulting in the spontaneous deletion of the marker, a loss of biological activity, or other effects that may not be well understood. Scientists would not tolerate introduc-

ing such unknown variables into their research. Finally, a scientifically trained bioterrorist could probably detect and remove an inserted DNA marker.[76]

Control of Transfers and Exports

Every country that transfers listed pathogens and toxins across national borders should establish rules for the safe and secure shipping of dangerous goods and import-export controls, and create a national body to enforce these regulations if one does not already exist. The United States and other Western industrialized countries view export controls as an essential means to prevent rogue states and terrorist organizations from acquiring the equipment, materials, and know-how needed to produce biological weapons. Although export controls are not a panacea and can be circumvented, they provide a way to slow down proliferation until other policy instruments can be brought to bear.

The United States has two parallel systems of national export controls. The Department of State oversees the International Traffic in Arms Regulations, which apply to the export of armaments, military technology, and technological information on the Munitions Control List. The Department of Commerce implements the Export Administration Regulations, which ban the export without a license of dual-use commercial goods, technology, and technological information on the Commerce Control List.[77] Existing export controls on dangerous pathogens have a number of loopholes, however. For example, the Department of Commerce requires export licenses for DNA strands that are "associated with pathogenicity," whether they have been extracted from microorganisms or synthesized from scratch; however, this definition is vague and subject to interpretation. Responsibility for deciding if a particular DNA sequence fits the definition rests with the exporter, and the rule can be easily circumvented by selling small pieces of viral DNA that are individually harmless but become pathogenic when assembled in the right order.[78] The Department of Commerce should clarify these regulations so as to reduce the risk of deliberate circumvention without imposing an undue burden on legitimate scientists.

In addition to complying with permit and licensing requirements at the local, state, and federal levels, culture collections and other suppliers of dangerous pathogens should establish reliable mechanisms to verify that their customers have a legitimate need for the requested material. The recipient should be located at an institution where work on select agents has been approved, all necessary biosafety and biosecurity policies are in place, and the receiving laboratory is capable of controlling access and screening potential users. Suppliers should keep a detailed record of each transaction, including the material sent (with strain and batch numbers where appropriate), the method and date of shipment, and the name and address of the recipient.

One issue that is bound to be highly controversial is whether countries that have implemented biosecurity standards would have an automatic right to receive transfers of dangerous pathogens from other participating states. A number of developing countries, including China, India, Iran, and Pakistan, have criticized the Australia Group (AG) controls on pathogen exports as discriminatory because they impede the development of commercial biotechnology industries in the targeted countries. Nevertheless, the United States and other AG members reserve the right to bar government, academic, and com-

mercial entities from transferring dangerous pathogens to countries that are either not parties to the BWC or are suspected of engaging in activities prohibited by the treaty.

Registration and Licensing of Facilities

Biosecurity standards should establish procedures for the registration and licensing of research laboratories and culture collections that possess, work with, or transfer listed pathogens and toxins. Registered facilities would be required to clean out their laboratory freezers and prepare a complete inventory of stored cultures. During the inventory process, vials would either be discarded or their contents verified. Although private industry has been fairly diligent about pathogen accounting, many academic centers do not have well-inventoried culture collections. Scientists tend to be poor librarians and often deposit personal samples in a laboratory freezer, leaving them untouched for years. When these individuals change jobs or retire, their poorly documented specimens remain behind. Despite the costs associated with conducting freezer inventories, this type of housekeeping is long overdue.

An important element of biosecurity is the periodic inspection by national authorities of laboratories that work with select agents. Individuals found in violation of the rules should be penalized with loss of pay, fines, suspension, or dismissal, depending on the seriousness of the infraction. Institutions found noncompliant should be assessed fines, suspension of a license, or loss of government funding. [79]

Physical Security Measures

Physical security measures are designed to prevent unauthorized entry into a laboratory and the removal of select agents that may be stored there. Implementing such measures poses the greatest challenge for academic institutions, which are the least familiar with them. In contrast, most commercial pharmaceutical or biotechnology companies are comfortable with site security because it is key to protecting their intellectual property and business secrets.

The level of physical protection at a facility should be commensurate with the level of hazard or threat associated with the pathogens it houses. Accordingly, the most dangerous agents and strains—from the standpoint of public-health impact and suitability for weaponization—should have the greatest restrictions on access and use. For some agents, however, the appropriate level of biosecurity does not track directly with biosafety level. Although certain toxins (such as ricin) are relatively safe to work with, requiring only BSL-2 biocontainment, they may pose a significant bioterrorist threat.[80] Salerno and his colleagues at Sandia National Laboratories have also identified a number of secondary assets that warrant physical protection, including technical information on pathogens and laboratory security systems, personnel files of individuals who work with listed agents or on lab security, and control systems involved in facility access, computer networks, and biocontainment.[81]

The Canadian Science Centre for Human and Animal Health in Winnipeg, Manitoba, is the world's only maximum-containment (BSL-4) facility that handles both human and animal pathogens. First opened in 1998, this laboratory has a state-of-the-art security system that cost $1 million to install, and the center spends an additional $650,000 per

year on guards and technology upgrades. Roughly a thousand intrusion-detection devices (for example, motion detectors, closed-circuit television cameras, and controlled doors) are scattered throughout the facility; the higher the sensitivity of an area, the greater the number of physical barriers protecting it. Access-control systems incorporating biometrics—security devices based on a unique physical characteristic, such as a fingerprint or a retinal scan—keep out unauthorized personnel.[82] Nevertheless, such high-technology solutions may not be affordable or appropriate for small university labs or facilities in developing countries.

Another limitation of physical security is that while access controls and locked doors can work against intruders from outside, they are much less effective against trusted insiders. It is particularly difficult to safeguard pathogens when they are being actively cultivated or experimented with at the laboratory bench. Indeed, this is the most vulnerable area for the covert theft or diversion of pathogens: no obvious technical or procedural method can prevent a motivated insider from removing small amounts of biological material in a small vial or even on an article of clothing. The fact that biological materials do not give off signatures that can be detected at a distance rules out the portal monitors employed in nuclear plants.

Nuclear-weapon facilities routinely employ the two-person rule: no staff member is allowed to handle fissile materials without being accompanied and observed by at least one other person. This procedure reduces the risk of diversion unless two authorized individuals are working in collusion, which is unlikely. Application of the two-person rule to microbiological facilities makes sense for research with the most dangerous pathogens, such as smallpox virus. The rule should not be widely applied, however, because it would be costly and awkward to implement. Having one lab worker observe another full-time would have the effect of doubling personnel costs; other drawbacks include crowding, an increased risk of laboratory accidents, and the possible exposure of the observer to the infectious agent. Subjecting scientists to continuous surveillance by closed-circuit television would also be impractical and probably ineffective. Given the limitations on the ability of physical security and inventory control measures to prevent the diversion of pathogens by trusted insiders, any system for restricting access to biohazardous materials must ultimately rely on personnel screening.

Screening of Laboratory Personnel

Because a security threat could arise from a permanent staff member or visiting scientist who takes advantage of privileged access to select agents, the best line of defense is to ensure the personal integrity and reliability of all such individuals. Senior laboratory officials are responsible for controlling who has access to pathogens. Background checks, such as verifying an individual's references and checking for a criminal history and ties to terrorist organizations, are an essential element of any biosecurity program. Staff members working in different parts of a high-containment facility may require different levels of vetting. According to guidelines developed by the U.S. Department of Agriculture, personnel working inside a BSL-3 facility but without direct access to pathogens must be checked against national law-enforcement and intelligence databases; staff members who have direct access to pathogens must have a partial background investigation; and those with pro-

gram-management responsibilities must have a full background investigation.[83] Because some reliability problems may not emerge until after an individual has been on the job for some time, personnel who have been granted unescorted access to pathogens should be subjected to periodic reinvestigation and drug testing.

Academic and industrial facilities working with listed pathogens have a responsibility to train scientists and technicians in good scientific practice, including biosafety and biosecurity. At a minimum, staff members need to know which individuals are authorized to enter a secure area and how to report suspected breaches of security. Because many institutions devote inadequate resources to training, young scientists may complete their graduate training with ingrained bad habits, increasing the risk of accidents and security breaches. Beyond training, it is important to instill in laboratory personnel a security culture that includes heightened awareness of the bioterrorism threat and vigilance in complying with biosecurity regulations.

Six

Conclusions

Drawing on best practices identified by the OECD Task Force on Biological Resource Centers and other international initiatives, states that are parties to the Biological Weapons Convention (BWC) should establish a technical working group for the negotiation of global biosecurity standards. Because of differences among legal systems, this working group should not attempt to develop model legislation but rather a set of detailed technical guidelines that can be converted into national regulations.

Developing biosecurity guidelines under the auspices of the BWC intersessional review process makes sense because it has already begun to address biosecurity issues. In addition to experts from BWC member-states, the proposed technical working group should include representatives of the World Health Organization (WHO), the Food and Agriculture Organization, and the World Organization for Animal Health. U.S. government officials have stated that they would prefer that the WHO, rather than a working group under BWC auspices, take the lead in developing biosecurity guidelines.[84] In the past, however, the WHO has tried to avoid politicization by defining itself as a public health and scientific organization and declining direct involvement in security or law enforcement issues. For this reason, the WHO would not be an optimal forum for negotiating a set of standards focused on biosecurity, as opposed to biosafety.

International Oversight Mechanism

Once countries have agreed on a set of biosecurity standards that can be incorporated into national laws and regulations, how will it be possible to ensure a reasonable degree of uniformity and accountability in implementation? A possible model for an international oversight mechanism is the Nuclear Safety Convention, which was negotiated under the auspices of the IAEA and adopted in Vienna on June 17, 1994. Parties to this treaty agree to apply basic safety guidelines to the location, design, construction, and operation of civilian nuclear power plants, including radiation protection, quality assurance, and emergency preparedness. To implement the agreed safety standards, each member-state is required to establish a nuclear regulatory agency that is effectively separate from the regulated industry and from government organizations that promote nuclear power.[85]

The Nuclear Safety Convention is an incentive instrument in that it does not enforce compliance through formal verification mechanisms such as on-site inspections, but rather through the common interest of the parties in achieving higher levels of nuclear plant safety. To this end, member-states submit periodic reports on steps they are taking to implement the safety guidelines. At regularly scheduled review meetings in Vienna, each participating state has an opportunity to discuss its own actions and to seek clarification of the progress reports submitted by others. Political pressure and the need for govern-

ments to appear responsible create incentives for countries to join the regime and comply with the agreed safety standards.

In much the same way, BWC member-states could convene annual biosecurity oversight meetings at which they are expected to report on the development and implementation of their national biosecurity systems and to answer questions from other participating countries. States that have failed to implement or adequately enforce the biosecurity regulations could be subjected to probing questions and political pressure during the annual meetings. To provide implementation assistance and to organize annual review meetings, a small international secretariat might be established. This entity could either be free-standing or linked to an existing international organization such as the WHO or the United Nations Educational, Scientific, and Cultural Organization (UNESCO).

Policy Recommendations

Efforts to develop and implement global biosecurity standards will involve a number of policy choices to ensure that the resulting guidelines are workable and cost-effective. Some recommendations follow:

Focus on strengthening the weakest links.
It would be counterproductive to develop biosecurity standards that are so complex and expensive that developing countries are financially and technically unable to implement them. Instead, the primary goal of an effort to create global standards should be to strengthen the weakest links—states whose research laboratories and pathogen collections are so poorly secured that terrorists could penetrate them fairly easily. One approach would be for countries to agree on a set of minimum performance benchmarks that can be met through a variety of different means, either labor-intensive or capital-intensive. Without improved procedures to ensure personnel reliability, for example, access-control security systems would be of limited value. In addition, developed countries should consider providing technical and economic assistance to developing countries, either on a multinational or bilateral basis, so that the minimum standards for the most problematic countries can be set higher than would otherwise be possible.

Engage the international scientific community in standards development.
The ultimate success of global biosecurity standards will depend on the cooperation of scientists and laboratory administrators around the world. Standards that are too rigid, bureaucratic, or costly to implement could deter academic or industrial scientists from engaging in vital biomedical or biodefense research with dangerous pathogens, and might lead them to destroy rare archival culture collections in the hope of avoiding regulatory costs or legal liability. Overly burdensome regulations could also motivate scientists to engage in informal exchanges of pathogens, defeating the very purpose of the new rules. For these reasons, the regulatory guidelines should be developed from bottom-up with the active participation of leading scientific organizations, rather than being imposed from top-down. To ensure that biosecurity standards are both practical and cost-effective, the technical working group should include representatives from international scientific orga-

nizations such as the International Union of Microbiological Societies (which has member societies in sixty-five countries) and the InterAcademy Panel on International Issues (a forum through which eighty national academies of science worldwide bring together leading authorities in the natural and social sciences to address scientific issues of international concern).[86]

Balance flexibility and uniformity.
Global biosecurity standards should be flexible enough to be tailored to individual facilities, yet sufficiently detailed to ensure a reasonable degree of consistency and uniformity in implementation. The standards must also reflect a balance of costs and risks, given that almost all pathogens can be isolated from the natural environment with a greater or lesser degree of effort. Excessively rigid standards could force institutions to invest in costly security equipment that is unnecessary or inappropriate, yet standards that are too vague could enable institutions to evade their biosecurity obligations. Another problem is that whereas regulations tend to be fixed and static, biological science and technology are in constant flux. Accordingly, a workable system of biosecurity standards must include a feedback mechanism and a streamlined amendment process so that select agent lists and security guidelines can be updated rapidly in response to advances in scientific knowledge and security technology. Moreover, any list of select agents should not be incorporated verbatim into national legislation, which would make it nearly impossible to modify.

Encourage participation and compliance through "carrots" rather than "sticks."
It is cheaper and easier to promote international compliance with biosecurity standards by means of incentives rather than some type of international policing mechanism. As noted above, the OECD's planned network of Biological Resource Centers will be an exclusive club whose benefits can be obtained only by meeting fairly demanding requirements for membership. This system will generate a strong positive motivation to adopt and comply with the agreed rules. In much the same way, eligibility for technical assistance provided by the WHO and other international organizations might be conditioned on states' having been certified as compliant with global biosecurity standards. Many developing countries are more concerned with natural epidemics of infectious disease than with bioterrorism, which is chiefly a preoccupation of the United States and other Western industrialized states. Nevertheless, developing nations should be willing to implement biosecurity standards in exchange for international financial and technical assistance in the struggle against infectious scourges such as HIV/AIDS, malaria, and tuberculosis.

Reconcile national biosecurity regulations with international arms control objectives.
Ensuring that pathogens are used only for peaceful purposes would help to strengthen the legal and ethical norms in the BWC against the development, production, and stockpiling of biological weapons. At the same time, biosecurity standards, which focus primarily on preventing bioterrorism, should be linked to efforts to promote state-level compliance with the BWC. For example, biosecurity measures should be designed so that they do not unduly reduce the transparency of national biodefense programs. The line between defensive and offensive work on biological weapons is inevitably somewhat blurred because

researchers must use dangerous pathogens to assess threats and test the effectiveness of detectors and countermeasures. Given this inherent ambiguity, excessive security at biodefense laboratories could arouse suspicion that supposedly defensive activities are being used as a cover for the development of biological weapons. For this reason, it is essential that biosecurity technologies and procedures be compatible with a reasonable level of transparency of biodefense research programs (without forcing states to reveal critical vulnerabilities that could render their defenses ineffective).

In conclusion, the development of global biosecurity standards would represent two notable departures from arms control as it has been traditionally practiced. First, rather than creating a legally binding treaty that is subject to intrusive verification (such as the Chemical Weapons Convention), biosecurity standards would be negotiated internationally but implemented through national legislation, with some oversight at the international level through periodic review meetings of the participating countries. Second, instead of focusing on the state-level proliferation of biological weapons, global biosecurity standards would reduce the risk of theft or diversion of pathogens by terrorists and criminals—a problem that the BWC does not explicitly address. Although biosecurity standards would not directly strengthen state-level compliance with the treaty, they would reinforce the basic norms enshrined within it. At the same time, biosecurity standards should be designed in such a way as to permit the future negotiation of a comprehensive, legally binding instrument to strengthen the BWC when the political environment for such an agreement becomes more favorable.

Appendix

Dangerous Pathogens and Toxins Subject to U.S. Federal Regulations

HHS NON-OVERLAP SELECT AGENTS AND TOXINS

Crimean-Congo haemorrhagic fever virus
Coccidioides posadasii
Ebola viruses
Cercopithecine herpesvirus 1 (Herpes B virus)
Lassa fever virus
Marburg virus
Monkeypox virus
Rickettsia prowazekii
Rickettsia rickettsii

South American haemorrhagic fever viruses

Junin
Machupo
Sabia
Flexal
Guanarito

Tick-borne encephalitis complex (flavi) viruses

Central European tick-borne encephalitis
Far Eastern tick-borne encephalitis
Russian spring and summer encephalitis
Kyasanur forest disease
Omsk hemorrhagic fever

Variola major virus (Smallpox virus)
Variola minor virus (Alastrim)
Yersinia pestis
Abrin
Conotoxins
Diacetoxyscirpenol
Ricin
Saxitoxin
Shiga-like ribosome inactivating proteins
Tetrodotoxin

HIGH CONSEQUENCE LIVESTOCK PATHOGENS AND TOXINS/SELECT AGENTS (OVERLAP AGENTS)

Bacillus anthracis
Brucella abortus
Brucella melitensis
Brucella suis
Burkholderia mallei (formerly *Pseudomonas mallei)*
Burkholderia pseudomallei (formerly *Pseudomonas pseudomallei)*
Botulinum neurotoxin producing species of *Clostridium*

Coccidioides immitis
Coxiella burnetii
Eastern equine encephalitis virus
Hendra virus
Francisella tularensis
Nipah Virus
Rift Valley fever virus
Venezuelan equine encephalitis virus
Botulinum neurotoxin
Clostridium perfringens epsilon toxin
Shigatoxin
Staphylococcal enterotoxin
T-2 toxin

USDA HIGH CONSEQUENCE LIVESTOCK PATHOGENS AND TOXINS (NON-OVERLAP AGENTS AND TOXINS)

Akabane virus
African swine fever virus
African horse sickness virus
Avian influenza virus (highly pathogenic)
Blue tongue virus (Exotic)
Bovine spongiform encephalopathy agent
Camel pox virus
Classical swine fever virus
Cowdria ruminantium (Heartwater)
Foot and mouth disease virus
Goat pox virus
Lumpy skin disease virus
Japanese encephalitis virus
Malignant catarrhal fever virus (Exotic)
Menangle virus
Mycoplasma capricolum/M.F38/*M. mycoides capri*
Mycoplasma mycoides mycoides
Newcastle disease virus (VVND)
Peste Des Petits Ruminants virus
Rinderpest virus
Sheep pox virus
Swine vesicular disease virus
Vesicular stomatitis virus (Exotic)

LISTED PLANT PATHOGENS

Liberobacter africanus
Liberobacter asiaticus
Peronosclerospora philippinensis
Phakopsora pachyrhizi
Plum Pox Potyvirus
Ralstonia solanacearum race 3, biovar 2
Schlerophthora rayssiae var zeae
Synchytrium endobioticum
Xanthomonas oryzae
Xylella fastidiosa (citrus variegated chlorosis strain)

Notes

1. W. Seth Carus, "The Rajneeshees (1984)," in Jonathan B. Tucker, ed., *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons* (Cambridge, Mass.: MIT Press, 2000), 115–37.

2. Barton Gellman, "Al Qaeda Near Biological, Chemical Arms Production," *Washington Post,* March 23, 2003, A1.

3. Stephen S. Morse, Mailman School of Public Health, Columbia University, presentation at National Academy of Sciences symposium on "Scientific Openness and National Security," Washington, D.C., January 9, 2003.

4. Sandra Fry, "Integrating Security and Biosafety: Developing a Biosecurity Program at the Canadian Food Inspection Agency" (presentation at the American Biological Safety Association [ABSA] conference on "Biosecurity: Challenges and Applied Solutions for Our Future Needs," Alexandria, Va., April 22, 2003).

5. U.S. Department of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention and National Institutes of Health, *Biosafety in Microbiological and Biomedical Laboratories,* 4th ed. (Washington, D.C.: U.S. Government Printing Office, May 1999).

6. Reuters, "Report Finds Easy Lab Access to Deadly Pathogens," May 8, 2002.

7. Rick Weiss and Joby Warrick, "Army Lost Track of Anthrax Bacteria: Specimens at Md.'s Fort Detrick May Have Been Misplaced or Stolen," *Washington Post,* January 21, 2002, A1; Charles Pillar, "Biodefense Lab Under a Microscope," *Los Angeles Times,* February 12, 2003, A1.

8. Elizabeth Williamson, "Lack of Lab Space May Delay New Vaccines," *Washington Post,* March 12, 2003, A19.

9. Dee Ann Davis and Nicholas M. Horrock, "Living Terror Part 1: Deadly Laboratories," United Press International, July 2, 2003.

10. David Dishneau, "Fort Detrick, NIH Outline Billion-Dollar Biodefense Complex," Associated Press, October 15, 2002.

11. Paul Elias, "Bush Bioweapons Push Worries Some," Associated Press, March 29, 2003.

12. Eileen Choffnes, "Bioweapons: New Labs, More Terror?" *Bulletin of the Atomic Scientists* 58, no. 5 (September/October 2002), 28–32.

13. Jonathan B. Tucker, "Preventing Terrorist Access to Dangerous Pathogens: The Need for International Biosecurity Standards," *Disarmament Diplomacy,* no. 66 (September 2002), 8–12.

14. Jenni Rissanen, "Continued Turbulence over BWC Verification," in Verification Research, Training, and Information Centre, *Verification Yearbook 2002* (Basford, UK: Russell Press, 2002), 75–89.

15. "Decision of the Fifth Review Conference of the Parties to the Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological)

Weapons and on Their Destruction," BWC/CONF.V/17, United Nations Office in Geneva, November 22, 2002, paras. 18–20.

16. Michael Barletta, Amy Sands, and Jonathan B. Tucker, "Keeping Track of Anthrax: The Case for a Biosecurity Convention," *Bulletin of the Atomic Scientists* 58, no. 3 (May/June 2002), 47–62.

17. Paul Keim, et al., "Molecular Evolution and Diversity in *Bacillus anthracis* as Detected by Amplified Fragment Length Polymorphism Markers," *Journal of Bacteriology* 179, no. 3 (February 1997): 818–24.

18. For a list of dangerous pathogens sold to Iraq in the 1980s, see U.S. Senate Committee on Banking, Housing, and Urban Affairs, *United States Dual-Use Exports to Iraq and Their Impact on the Health of the Persian Gulf War Veterans.* Hearing before the Committee on Banking, Housing, and Urban Affairs, United States Senate, 103rd Cong., 2nd sess., May 25, 1994 (Washington, D.C.: U.S. Government Printing Office, 1994), 266–75.

19. National Commission on Terrorism, *Countering the Changing Threat of International Terrorism* (Washington, D.C.: U.S. Government Printing Office, June 5, 2000).

20. Gary K. Bertsch, et al., *The Human Factor and Security Culture: Challenges to Safeguarding Fissile Materials in Russia* (Athens, Ga.: Center for International Trade and Security, University of Georgia, November 2002), 7–8.

21. Ibid.

22. American Biological Safety Association, "ABSA Biosecurity Task Force White Paper: Understanding Biosecurity," *Applied Biosafety* 7, no. 2 (2002), 97.

23. Ronald J. Jackson, et al., "Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox," *Journal of Virology* 75, no. 3 (February 2001): 1205–10.

24. Jeronimo Cello, Aniko V. Paul, and Eckhard Wimmer, "Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template," *Science* 297 (August 9, 2002), 1016–18. See also, Rick Weiss, "Polio-Causing Virus Created in N.Y. Lab: Made-From-Scratch Pathogen Prompts Concern About Bioethics, Terrorism," *Washington Post,* July 12, 2002, A1.

25. American Biological Safety Association, "ABSA Biosecurity Task Force White Paper," 96.

26. Rick Weiss, "Ordering Germs? There Are Hurdles First," *Washington Post,* October 12, 2001, A27.

27. Jessica Eve Stern, "Larry Wayne Harris (1998)," in Tucker, ed., *Toxic Terror,* 227–46.

28. Stephen A. Morse, U.S. Centers for Disease Control and Prevention, "The New Select Agent Regulation" (presentation at the ABSA conference on "Biosecurity: Challenges and Applied Solutions for Our Future Needs," Alexandria, Va., April 22, 2003).

29. The current list of states that sponsor terrorism includes Iraq, Iran, Libya, Syria, Cuba, North Korea, and Sudan.

30. Bernadette Tansey, "U.S. Requires Scientists to Give FBI Fingerprints: Thousands Who Use Bioterror Compounds Must Disclose Data for Background Checks," *San Francisco Chronicle,* March 12, 2003, A3.

31. Diana Jean Schemo, "Sept. 11 Strikes at Labs' Doors," *New York Times,* August 13, 2002, F1.

32. Associated Press, "Government Issues Guidelines to Tighten Laboratory Security," December 6, 2002.

33. 42 Code of Federal Regulations (CFR), Part 73, "Possession, Use, and Transfer of Select Agents and Toxins" [Interim Final Rule], *Federal Register,* vol. 240, no. 67 (December 13, 2002), pp. 76886–905.

34. Reynolds M. Salerno, Sandia National Laboratories, personal communication, May 26, 2003.

35. 42 CFR, Part 73, "Possession, Use, and Transfer of Select Agents and Toxins," p. 76902.

36. "Keeping Track of Biological Agents," *Trust & Verify,* no. 106 (January–February 2003), 106–107.

37. Jonathan Y. Richmond and Shanna L. Nesby-O'Dell, "BMBL Appendix F: Laboratory Security and Emergency Response Guidance for Laboratories Working with Select Agents," supplement, *Morbidity and Mortality Weekly Report,* vol. 51, no. RR19;1 (December 6, 2002), available at www.cdc.gov/od/ohs/biosfty/bmbl4/b4af.htm.

38. Douglas Moore, Office of Safety and Health, Plum Island Animal Disease Center, "Biosecurity Implementation at a Biologically Secure Facility" (presentation at the ABSA conference on "Biosecurity: Challenges and Applied Solutions for Our Future Needs," Alexandria, Va., April 22, 2003).

39. Debra Hunt, Division of Biological Safety, Duke University, "Impact of Biosecurity on Biomedical Research at Duke University" (presentation at the ABSA conference on "Biosecurity: Challenges and Applied Solutions for Our Future Needs," April 22, 2003).

40. American Society for Microbiology, "ASM Comments on Interim Rule," available at www.asmusa.org.

41. American Society for Microbiology, "List of Currently Known BSL-4 Facilities Worldwide." Online. Available: www.asmusa.org/memonly/asmnews/nov99/figs/t1f1.htm. (Accessed October 8, 2002.)

42. Ken Alibek with Stephen Handelman, *Biohazard* (New York: Random House, 1999).

43. Kara Yermukan, memorandum on "Trip Report: Interview with Professor Igor V. Domaradsky, Moscow," Center for Nonproliferation Studies, Monterey, Calif., September 2002.

44. Cable News Network, "Concern Over Kazakhstan Bio-Theft Bid," November 5, 2002.

45. Joby Warrick, "Biotoxins Fall into Private Hands," *Washington Post,* April 21, 2003, A1.

46. William J. Broad, "Obtaining Anthrax Is Hard, But Not Impossible," *New York Times,* October 10, 2001, B12.

47. Michael Barletta, "Biosecurity Measures for Preventing Bioterrorism," Center for Nonproliferation Studies, Monterey Institute of International Studies, November 27, 2002.

48. Council of the European Union, "Action Plan for the Implementation of the Basic Principles for an EU Strategy Against Proliferation of Weapons of Mass Destruction." Document 10254/1/03. Brussels, June 13, 2003, 9.

49. Peter Eisler, "U.S., Russia Tussle over Deadly Anthrax Sample," *USA Today,* August 19, 2002, 1–2.

50. William J. Broad, "World's Largest Germ-Bank Union Acts to Keep Terrorists From Stealing Deadly Stocks," *New York Times,* October 23, 2001, B9.

51. World Data Centre for Microorganisms, "Culture Collection Organization Statements on Biological Warfare." Online. Available: wdcm.nig.ac.jp/announce.html. (Accessed March 25, 2003.)

52. European Culture Collections Organization, "Prevention of Proliferation of Dangerous Microorganisms – The ECCO Principles." Online. Available: www.eccosite.org/prevention.htm. (Accessed March 25, 2003.)

53. Organization for Economic Cooperation and Development, *Biological Resource Centers: Underpinning the Future of Life Sciences and Biotechnology* (Paris: OECD, March 2001).

54. Scott Stern, *Biological Resource Centers: Knowledge Hubs for the Life Sciences* (Washington, D.C.: Brookings Institution Press, 2003).

55. Telephone interview with Melissa P. Horwitz, science and social policy adviser, U.S. Mission to the OECD, November 27, 2002.

56. Telephone interview with Iaian Gillespie, OECD, March 20, 2003.

57. Ibid.

58. Ibid.

59. "Statement of G7 Health Ministers' Meeting, Ottawa, Canada, November 7, 2001." University of Toronto, G8 Information Center. Online. Available: www.g8.utoronto.ca/health/ottawa2001.html. (Accessed April 24, 2003.)

60. "Statement of G7 Health Ministers' Meeting [with Mexico], London, March 14, 2002." University of Toronto, G8 Information Center. Online. Available: www.g8.utoronto.ca/health/ottawa2001.html. (Accessed April 24, 2003.)

61. Interview with Stefan Wegener, Canadian Science Centre for Human and Animal Health, Winnipeg, Manitoba, July 7, 2003.

62. Current members of the Australia Group are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Cyprus, Czech Republic, Denmark, European Commission, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, South Korea, Luxembourg, the

Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

63. Jonathan Yang, "Australia Group Adds 14 Pathogens to Control List," *Arms Control Today* 33, no. 6 (July/August 2003), 31.

64. Lois R. Ember, "Stemming the Tide: Australia Group Adopts Guidelines, Tightens Export Controls on Chemical, Biological Arms," *Chemical & Engineering News,* July 15, 2002, 28.

65. "News Chronology: 3-6 June," *CBW Conventions Bulletin,* no. 57 (September 2002), 36.

66. U.S. Department of State, "Fact Sheet Shows U.S. Efforts to Combat Biological Weapons Threat," Washington, D.C., November 14, 2002.

67. Thomas Cueni, secretary-general, Interpharma: The Association of Pharmaceutical Research Companies of Switzerland, "Draft: Biosafety and Biosecurity – Industry Best Practices to Prevent Misuse of Biohazardous Material," Basel, Switzerland, May 2002.

68. American Biological Safety Association, "ABSA Biosecurity Task Force White Paper," 96.

69. Reynolds M. Salerno, Natalie Barnett, and Jennifer G. Koelm, "Balancing Security and Research at Biomedical and Bioscience Laboratories." No. 2003-0701C. Sandia National Laboratories, Albuquerque, March 2003, 7.

70. Telephone interview with D. Jay Grimes, provost, University of Southern Mississippi, March 25, 2003.

71. Lisa D. Rotz, Ali S. Khan, Scott R. Lillibridge, Stephen M. Ostroff, and James M. Hughes, "Public Health Assessment of Potential Biological Terrorism Agents," *Emerging Infectious Diseases* 8, no. 2 (February 2002), 225–30.

72. Salerno, Barnett, and Koelm, "Balancing Security and Research," 6.

73. Gerald L. Epstein, U.S. Defense Threat Reduction Agency, Washington, D.C., personal communication, May 19, 2003.

74. Rick Weiss, "Mail-Order Molecules Brew a Terrorism Debate," *Washington Post,* July 17, 2002, A1.

75. Paul Keim, *Microbial Forensics: A Scientific Assessment* (Washington, D.C.: American Academy of Microbiology, 2003), 16. For an example of tracking the source of a pathogen used in a bioterrorist attack by measuring levels of naturally occurring radioisotopes whose concentration varies according to geographical location (in this case, the amount of the rare isotope oxygen 18, which is more concentrated in sea water than fresh water and thus tends to be more plentiful in bacteria that grow near coastlines), see William J. Broad, "F.B.I. Names Top Scientists for Advisory Panel on Germs," *New York Times,* September 26, 2003, A20.

76. Interview with Stephen S. Morse, Mailman School of Public Health, Columbia University, New York, November 20, 2002.

77. Because the Export Administration Act of 1979 was not reauthorized by Congress in 2002, President George W. Bush invoked the International Economic Emergency Powers Act to maintain regulations on exports of dual-use technologies under the Export Administration Regulations.

78. Weiss, "Mail-Order Molecules Brew a Terrorism Debate."

79. Amy E. Smithson, ed., *Compliance Through Science: U.S. Pharmaceutical Industry Experts on a Strengthened Bioweapons Nonproliferation Regime.* Report No. 48 (Washington, D.C.: Henry L. Stimson Center, September 2002), 44–45.

80. Sandra Fry, Canadian Food Inspection Agency, "Integrating Security and Biosafety" (presentation at the ABSA conference on "Biosecurity: Challenges and Applied Solutions for Our Future Needs," Alexandria, Va., April 22, 2003).

81. Salerno, Barnett, and Koelm, "Balancing Security and Research," 7.

82. Kevin Smith, Manager, Security Operations, Canadian Science Centre for Human and Animal Health, "Biosafety and Biosecurity: Lessons Learned at the Canadian Science Centre for Human and Animal Health" (presentation at the ABSA conference on "Biosecurity: Challenges and Applied Solutions for Our Future Needs," Alexandria, Va., April 22, 2003).

83. Douglas M. Moore, "A Summary: USDA Security Policies and Procedures for Biosafety Level 3 Facilities," *Applied Biosafety* 7, no. 2 (2002), 100.

84. Lois Ember, "Securing Deadly Pathogens," *Chemical & Engineering News* 81, no. 26 (June 30, 2003), 25.

85. Carl E. Behrens and Warren H. Donnelly, "The Convention on Nuclear Safety—A Fact Sheet." CRS Report, No. 96-434 ENR, Washington, D.C., Congressional Research Service, May 16, 1996.

86. Information on the International Union of Microbiological Societies is available at www.iums.org. Information on the InterAcademy Panel is available at www.InterAcademies.net.

About the Author

Jonathan B. Tucker is a senior researcher specializing in chemical and biological weapons issues at the Center for Nonproliferation Studies at the Monterey Institute of International Studies, where he has worked since March 1996. Previously, he was a senior policy analyst for the Presidential Advisory Committee on Gulf War Veterans' Illnesses (1995), a biological weapons inspector with the UN Special Commission on Iraq (1995), a specialist in chemical arms control at the United States Arms Control and Disarmament Agency (1993–1995), and a weapons analyst at the congressional Office of Technology Assessment (1990–1993). Tucker has received fellowships from Stanford University's Hoover Institution (1999–2000), the American Association for the Advancement of Science (1989–1990), the Ford Foundation (1988–1989), and the Robert Bosch Foundation (1987–1988). His most recent book is *Scourge: The Once and Future Threat of Smallpox.* He also edited T*oxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons.* He holds a Ph.D. in political science from the Massachusetts Institute of Technology and a B.S. in biology from Yale University. He was a senior fellow at the United States Institute of Peace in 2002–2003.

About the Institute

The **United States Institute of Peace** is an independent, nonpartisan federal institution created by Congress to promote the prevention, management, and peaceful resolution of international conflicts. Established in 1984, the Institute meets its congressional mandate through an array of programs, including grants, fellowships, professional training, education programs from high school through graduate school, conferences and workshops, library services, and publications. The Institute's Board of Directors is appointed by the President of the United States and confirmed by the Senate.

Chairman of the Board: Chester A. Crocker
Vice Chairman: Seymour Martin Lipset
President: Richard H. Solomon
Executive Vice President: Harriet Hentges
Vice President: Charles E. Nelson

Board of Directors

Chester A. Crocker (Chairman), James R. Schlesinger Professor of Strategic Studies, School of Foreign Service, Georgetown University

Seymour Martin Lipset (Vice Chairman), Hazel Professor of Public Policy, George Mason University

Betty F. Bumpers, Founder and former President, Peace Links, Washington, D.C.

Holly J. Burkhalter, Advocacy Director, Physicians for Human Rights, Washington, D.C.

Charles Horner, Senior Fellow, Hudson Institute, Washington, D.C.

Stephen D. Krasner, Graham H. Stuart Professor of International Relations, Stanford University

Marc E. Leland, Esq., President, Marc E. Leland & Associates, Arlington, Va.

Mora L. McLean, Esq., President, Africa-America Institute, New York, N.Y.

María Otero, President, ACCION International, Boston, Mass.

Daniel Pipes, Director, Middle East Forum, Philadelphia, Pa.

Barbara W. Snelling, Former State Senator and former Lieutenant Governor, Shelburne, Vt.

Harriet Zimmerman, Vice President, American Israel Public Affairs Committee, Washington, D.C.

Members ex officio

Lorne W. Craner, Assistant Secretary of State for Democracy, Human Rights, and Labor

Michael M. Dunn, Lieutenant General, U.S. Air Force; President, National Defense University

Douglas J. Feith, Under Secretary of Defense for Policy

Richard H. Solomon, President, United States Institute of Peace (nonvoting)

Other titles in the Peaceworks series

Healing the Holy Land: Interreligious Peacebuilding in Israel/Palestine, by Yehezkel Landau (No. 51, August 2003)

Boundary Disputes in Latin America, by Jorge I. Domínguez with David Mares, Manuel Orozco, David Scott Palmer, Francisco Rojas Aravena, and Andrés Serbin (No. 50, August 2003)

The Road Ahead: Lessons in Nation Building from Japan, Germany, and Afghanistan for Postwar Iraq, by Ray Salvatore Jennings (No. 49, May 2003)

The Palestinian Reform Agenda, by Nathan Brown (No. 48, December 2002)

The Israeli Military and Israel's Palestinian Policy: From Oslo to the Al Aqsa Intifada, by Yoram Peri (No. 47, November 2002)

The Chaplain's Evolving Role in Peace and Humanitarian Relief Operations, by Captain Paul McLaughlin (No. 46, September 2002)

The Ethics of Armed Humanitarian Intervention, by C. A. J. Coady (No. 45, July 2002)

Democratic Values, Political Structures, and Alternative Politics in Greater China, by David Zweig (No. 44, June 2002)

Training for Peace and Humanitarian Relief Operations: Advancing Best Practices, by Robert M. Schoenhaus (No. 43, April 2002)

The Role of International Financial Institutions in International Humanitarian Law, by Laurie R. Blank (No. 42, January 2002)

Controlling Weapons of Mass Destruction: Findings from USIP-Sponsored Projects, edited by Deepa M. Ollapally (No. 41, September 2001)

Passing the Baton: Challenges of Statecraft for the New Administration, with remarks by Samuel R. Berger and Condoleezza Rice (No. 40, May 2001)

From Revolutionary Internationalism to Conservative Nationalism: The Chinese Military's Discourse on National Security and Identity in the Post-Mao Era, by Nan Li (No. 39, May 2001)

El Salvador: Implementation of the Peace Accords, edited by Margarita S. Studemeister (No. 38, January 2001)

The News Media and Peace Processes: The Middle East and Northern Ireland, by Gadi Wolfsfeld (No. 37, January 2001)

Conflict Management Training: Advancing Best Practices, by Robert M. Schoenhaus (No. 36, January 2001)

Coercive Prevention: Normative, Political, and Policy Dilemmas, by Bruce W. Jentleson (No. 35, October 2000)

Women in War and Peace: Grassroots Peacebuilding, by Donna Ramsey Marshall (No. 34, August 2000)

Grappling with Peace Education in Serbia, by Ruzica Rozandic (No. 33, April 2000)

OF RELATED INTEREST

Other publications from the United States Institute of Peace address issues of direct relevance to international terrorism and security.

Recent Institute reports include:

The Diplomacy of Counterterrorism: Lessons Learned, Ignored, and Disputed (Special Report 80, January 2002)

Adapting to the New National Security Environment (Special Report 64, December 2000)

How Terrorism Ends (Special Report 48, May 1999)

To obtain an Institute report (available free of charge), please visit our web site (www.usip.org/reports). Or you can write United States Institute of Peace, 1200 17th Street NW, Suite 200, Washington, DC 20036-3011; call 202-429-3832; or fax 202-429-6063.

United States
Institute of Peace
1200 17th Street NW
Washington, DC 20036

Peaceworks 52