Preventing the Misuse of Pathogens: The Need for Global Biosecurity

Jonathan B. Tucker

The anthrax-tainted letters sent through the U.S. mail in the fall of 2001, infecting 22 people and killing five, hinted at the mayhem that could result from the large-scale release of a “weaponized” disease agent. Since then, efforts to counter bioterrorism have focused on the medical and public health response to an attack rather than on prevention. Although improved disease surveillance and therapeutic countermeasures are needed, it is also critical to impede biological attacks by making it more difficult for terrorists to obtain deadly pathogens and toxins (poisonous chemicals produced by living organisms).\(^1\)

Shortly after the anthrax mailings, the U.S. government tightened domestic regulations on access to hazardous biological materials that have legitimate uses in research and industry but could be misused by terrorists. The United States deserves credit for putting its domestic house in order, but no comparable security measures currently exist at thousands of research centers, clinical laboratories, and culture collections overseas that possess or work with dangerous pathogens and toxins. This lack of international harmonization has created security gaps that could be exploited by terrorists.

Negotiating global standards that restrict access to dangerous pathogens would reduce the threat of bioterrorism, while reinforcing the legal prohibitions on the development, production, and stockpiling of biological and toxin weapons contained in the 1972 Biological Weapons Convention (BWC). Since its inception, the credibility of the BWC has been undermined by its lack of formal mechanisms for monitoring and verification, and efforts over the past decade to strengthen the treaty have been largely unsuccessful. Although the BWC review conferences in 1986 and 1991 introduced politically binding confidence-building measures (CBMs) to increase transparency and improve compliance, only a minority of member states have submitted annual CBM reports. More recently, a six-year effort to negotiate a legally binding inspection protocol to supplement the BWC collapsed in July 2001 when the United States rejected the draft text.

The Bush administration views the terrorist acquisition and use of biological weapons as a more urgent threat than state-level proliferation, and it is also skeptical about the utility of legally binding multilateral agreements. Accordingly, the U.S. government has sought to bolster the BWC by urging member states to pass national legislation mandating domestic measures to counter 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 review conference in late 2006. The aim of these meetings is to “promote common understanding and effective action” on five measures that could be taken at the national level to strengthen the BWC: penal legislation, pathogen security measures, enhanced international procedures to investigate and mitigate the alleged use of biological weapons or suspicious outbreaks of infectious disease, improved mechanisms for global disease surveillance and response, and scientific codes of conduct.\(^2\)

The first experts meeting in Geneva on August 18-29, followed by the first meeting of BWC member states November 10-14, will address two issues: national implementation measures for the enactment of penal legislation and best practices for the security and oversight of pathogenic microorganisms and toxins. This article addresses the latter topic, which has come to be termed
“biosecurity.”

Defining “Biosecurity”

Although the terms “biosafety” and “biosecurity” are often used interchangeably, they refer to different issues. Biosafety technologies and procedures aim to prevent accidental infections of biomedical researchers and releases of dangerous pathogens from research laboratories that could endanger public health or the environment. These objectives can be achieved through “biocontainment,” which involves placing impermeable barriers or filters between the infectious agent and the researcher and between the laboratory and the outside world. Four levels of increasingly stringent biocontainment—referred to as Biosafety Levels (BSL) 1 through 4—are keyed to the lethality and contagiousness of pathogens and the availability of protective vaccines or therapeutic drugs.

Biosecurity, in contrast, denotes policies and procedures designed to prevent the deliberate theft, diversion, or malicious use of high-consequence pathogens and toxins. (A third term, “biosurety,” refers to the integration of biosafety and biosecurity.) In thinking about biosecurity, it is important to note some fundamental differences between biological and nuclear weapons materials (mainly plutonium and highly enriched uranium) that determine the effectiveness of controls. First, dangerous biological agents exist naturally in the environment. (The sole exception is the smallpox virus, which was eradicated from the wild in 1977 and is stored officially in only two repositories.) Second, since microorganisms will reproduce rapidly under the right conditions, large quantities can be grown from extremely small samples. Finally, biological materials have numerous civilian uses. (See Table 1.) Given the unique characteristics of pathogens, they cannot be controlled to the extent that nuclear weapons materials can be. As a result, it is necessary to develop a new security paradigm that is specifically tailored to microorganisms.

Although it is not possible to measure precisely the level of risk associated with poor security at microbiological laboratories, some recent incidents in the United States and elsewhere have hinted at the magnitude of the problem. A report in May 2002 by the inspector-general of the U.S. Department of Agriculture found that many of the department’s 124 research laboratories were vulnerable to theft and could not account accurately for their stocks of animal and plant pathogens. Similarly, investigations of the Pentagon’s leading biodefense facility, the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) at Fort Detrick, Maryland, found chronic problems with laboratory security during the 1980s and 1990s, including repeated failures to account for samples of pathogens because of poor internal controls and record-keeping.

If such concerns over laboratory security persist, the Bush administration’s plan for a massive increase in funding for biodefense research and development could prove counterproductive. The U.S. federal budget for fiscal year 2003 allocated more than $1.5 billion to the National Institutes of Health for work on bioterrorism countermeasures—a fivefold increase over the previous year. If the Bush administration gets its way, additional appropriations on this scale will continue for the next several years. Much of this money would be spent on the construction of new or expanded high-containment laboratories and related infrastructure for basic and applied research on dangerous pathogens. Ironically, the rapid expansion of biodefense research could create new security problems by multiplying many-fold the number of people with access to hazardous biological materials.

The Threat of Diversion

Until quite recently, controls on biological pathogens were driven more by concerns over safety than security. In contrast to the strict safeguards placed on nuclear weapons materials, dangerous pathogens and toxins have typically been stored in unprotected research laboratories and shipped across national borders with minimal precautions. University-based researchers have a long tradition of sharing microbial cultures informally through the mail, and few countries restrict who is granted access to infectious agents.

One reason for this laxity was that biological threats were not recognized to be as dangerous as nuclear threats, particularly in the pre-September 11 environment. Another reason is that most
pathogens and toxins can be obtained from natural sources. A skilled microbiologist can isolate a bacterium or virus from diseased animals, clinical specimens, and even from soil (in the case of anthrax spores). Nevertheless, reliance on these sources entails certain drawbacks. Since natural strains of pathogens vary widely in virulence, or the degree to which a microbe can cause disease, many of the strains isolated from nature could not be developed into effective weapons.

Given the technical difficulties associated with acquiring virulent microorganisms from natural sources, terrorists might well have a higher probability of success if they stole well-defined strains from a research facility, a clinical laboratory, a commercial supplier, or a state-owned culture collection or purchased such strains under false pretenses. The Ames and Vollum strains of anthrax, for example, are known to be highly virulent. Thus, the main purpose of biosecurity standards and procedures is to make it harder for terrorists to acquire deadly pathogens by making sure that legitimate activities and facilities are off-limits. Determined terrorists will then be forced to isolate virulent strains from natural sources, which are considerably less reliable.

Research laboratories working with dangerous pathogens face two main threats of theft or diversion: from outsiders and from insiders. In addition to criminal gangs and terrorist cells, outsiders could include visiting scientists, students, and short-term contractors who might attempt to steal pathogens covertly during a visit or stay at the facility. Insiders, in contrast, are trusted members of the scientific or technical staff who have been granted unescorted access and are familiar with laboratory security procedures and equipment. Such individuals might be motivated to steal dangerous pathogens for a variety of reasons, including resentment over being reprimanded or passed over for promotion, financial pressures, blackmail threats and other forms of external pressure, psychological or personal problems such as divorce or substance abuse, or recruitment by a terrorist organization.

The temptation to divert pathogens for sale on the black market might be particularly strong in the ex-Soviet states, where former bioweapons scientists currently receive only a fraction of their previous salary and perks. Traditional approaches to facility security such as “guns, gates, and guards” cannot prevent a covert outsider or a trusted insider from stealing a small sample of a pathogen and cultivating it in large quantities for illicit purposes. To prevent such misuse, biosecurity systems require an integrated approach that includes physical protection, access controls, materials accountability, and personnel screening.

The International Dimension

The United States currently leads all other countries in the extent and detail of its biosecurity legislation. Yet, even as the U.S. government implements the new regulations, the international dimension of the problem remains to be addressed. Several countries outside the United States have passed domestic laws that contain provisions on biosecurity, including Canada, France, Germany, Israel, Japan, and the United Kingdom. Nevertheless, many other countries conduct research on infectious disease agents such as anthrax and plague, maintain collections of microbial pathogens, and operate maximum-containment laboratories that handle the most deadly and incurable disease agents. Relying exclusively on nationally developed guidelines would result in an uneven patchwork of regulations, creating pockets of lax implementation or enforcement. For this reason, any effective campaign to restrict terrorist access to dangerous pathogens will have to be global in scope.

Roughly 1,500 state-owned and commercial culture collections worldwide maintain, exchange, and sell samples of microbes and toxins for scientific and biomedical research. These organizations vary widely in size and content, from large nonprofit organizations such as American Type Culture Collection to “boutique” collections based at universities, federal agencies, and private companies. About a third of the culture collections outside the United States might possess dangerous pathogens that are not adequately secured and controlled, making them vulnerable to theft or diversion. Trade in microbial cultures is also poorly regulated, both within countries and among them. In the United States, the Commerce Department licenses exports of pathogens and toxins on a list of “select agents,” and the Centers for Disease Control and Prevention authorizes imports. In many other countries, however, culture collections routinely ship dangerous pathogens with few questions asked.
The security situation in states with former offensive biowarfare programs is particularly troubling. During the late 1980s, some 60,000 scientists and technicians in the Soviet Union worked on biological weapons at more than 50 research institutes and production plants around the country. After the breakup of the Soviet Union in 1991, the old structures of authority and control collapsed, putting pathogen collections in the newly independent states of Russia, Kazakhstan, Uzbekistan, and Georgia at risk of theft or diversion by terrorists or criminals. In November 2002, authorities in Almaty, Kazakhstan, arrested a man who entered the Scientific Center for Quarantine and Zoonotic Diseases with the apparent intent of stealing samples of dangerous pathogens. Fortunately, the intruder was arrested before penetrating the second layer of physical security, which had only recently been upgraded with U.S. government assistance.\(^7\)

Another former biowarfare program that poses a proliferation threat is that of South Africa. Known as “Project Coast,” this program began in 1981 and focused on developing small-scale, custom-made weapons to terrorize and kill opponents of the apartheid regime. Project Coast scientists collected hundreds of deadly strains, including the causative agents of anthrax, brucellosis, cholera, and plague. After the program was dismantled in 1993, former Project Coast scientists secretly retained samples of virulent strains to continue work on vaccines and antidotes with commercial potential. They also attempted to sell cultures of deadly pathogens, including genetically engineered varieties, to the United States and possibly to other countries.\(^8\)

Although the World Federation for Culture Collections (WFCC) has urged its members to restrict the distribution of sensitive materials to third parties, the organization lacks the funding and authority needed to enforce compliance. Moreover, more than two-thirds of culture collections worldwide do not belong to the federation.\(^9\) Even if the WFCC recommendation could be enforced, it does nothing to set a minimum security standard and hence does not address the problem that weak regulations in some countries undercut more stringent efforts in others.

Since international terrorist organizations are likely to seek biowarfare materials from the most accessible source, international biosecurity standards would reduce the risk that terrorists could obtain dangerous pathogens from foreign laboratories and culture collections. Harmonized guidelines for transferring pathogens would also facilitate collaborative research and development on biodefense vaccines and drugs. Joint U.S.-Russian research projects on defenses against anthrax and smallpox, for example, have been hampered by incompatible national regulations on the export of dangerous pathogens.\(^10\)

**Developing a Biosecurity Regime**

An effective biosecurity system requires the integration of technologies and procedures. The global guidelines should include, as a minimum, the registration and licensing of facilities that work with dangerous biological agents, based on an agreed list of pathogens and toxins that can be readily updated; physical security and access controls at laboratories and culture collections that possess such agents; systems for the control and accounting of listed pathogens and toxins, both in storage and during experiments; background checks on laboratory personnel; and an emergency plan for responding to breaches in security. In view of the wide variety of facilities that work with hazardous biological materials, ranging from pharmaceutical companies to academic research labs, biosecurity measures cannot be developed on a “one size fits all” basis. According to a “white paper” by the American Biological Safety Association, guidelines for laboratory security should consist of functional requirements that the affected entities can implement in a tailored manner.\(^11\)

It is also important to balance the complexity and cost of biosecurity measures introduced at a facility against the threats posed by the pathogens and toxins that are actually held or used at the facility. To develop a tailored biosecurity plan, each entity that possesses or works with biohazardous materials should conduct a threat assessment of what assets need to be protected and the most likely diversion scenarios. Having identified the greatest risks, the facility should then do a vulnerability assessment based on how and where the pathogens or toxins are employed in research protocols, the security conditions under which they are stored and used, and how they are moved within the facility or transferred to outside locations. Given the impossibility of protecting all assets against all conceivable threats, laboratories must prioritize risks. Cost is an obvious limiting factor in
the choice of security measures, since small university laboratories cannot afford state-of-the-art systems such as biometric identifiers and computerized inventory systems.

Physical security poses the greatest challenge to academic institutions, which are the least familiar with it. Most commercial pharmaceutical firms have already implemented extensive site security measures to protect intellectual property and valuable business secrets. In general, the level of security should be commensurate with the level of risk, so that the most dangerous agents and strains—from the standpoint of public health impact and suitability for weaponization—are subjected to the highest levels of physical protection and access control. Nevertheless, biosecurity requirements do not always track directly with biosafety levels: some agents that require lower levels of biocontainment, such as toxins, might pose a significant bioterrorist threat. Reynolds Salerno and his colleagues at Sandia National Laboratories have also identified a number of “secondary assets” at biological research facilities that warrant protection, including detailed information about regulatory compliance and biosecurity programs, personnel records, and computer databases.

To augment physical security, facilities should establish procedures for the accountability of pathogens during their storage in a central repository and their utilization in laboratory experiments. Such procedures include conducting inventories and audits of sample collections, documenting the “chain of custody” of dangerous pathogens outside the access-controlled area, and verifying the destruction of working stocks at the end of an experiment. Any pathogen accountability system is unfortunately not foolproof; because microorganisms reproduce, a scientist who has access to a pathogen could covertly remove a small amount (taking steps to ensure that the organism remained alive and viable under the transport conditions) and later mass-produce it.

Academic and industrial facilities working with dangerous pathogens should train scientists and technicians in appropriate laboratory practice, including elements of both biosafety and biosecurity. Because scientists are not security experts, however, each facility that houses dangerous pathogens should employ a security professional to assess threats and vulnerabilities and develop a tailored biosecurity plan. Should a theft or diversion be detected, the incident must be reported promptly to the responsible government agency.

Given the inherent limitations on the ability of physical security and inventory control measures to prevent insider diversion or theft, any biosecurity system ultimately depends on the personal integrity and reliability of the laboratory staff. Background investigations are a critical element of any biosecurity program, including verifying an individual’s references and checking government or Interpol databases for a criminal history or links to terrorist organizations. Because reliability problems might not emerge until long after an individual has been hired, staff members who work with dangerous pathogens should be subjected to periodic reinvestigation, particularly before they are granted unescorted access to secure areas.

The final element of a biosecurity plan involves controls on transfers of dangerous pathogens, both domestic and international. Each country that ships listed pathogens and toxins across national borders should establish regulations for the safe and secure transportation of hazardous goods, controls on imports and exports, and verification of the declared end-use. A national export-control body should be established to enforce these regulations if one does not already exist. In addition to complying with permit and licensing requirements at the local, state, and federal levels, suppliers of biological pathogens should keep detailed records of each transaction, including strain and batch numbers, method and date of shipment, and name and address of each recipient. Suppliers should also establish reliable mechanisms to verify that recipients of pathogens and toxins have a legitimate need for the requested materials and that all necessary safety and security policies are in place.

Negotiation and Oversight

In preparation for the upcoming August meeting of the BWC experts group in Geneva, the U.S. government has circulated four short papers, two describing U.S. domestic legislation on penal legislation and biosecurity and two outlining how the BWC states-parties might proceed in these areas. The U.S. position on biosecurity is that the World Health Organization (WHO), the Food and
Agriculture Organization (FAO), and the World Organization for Animal Health (OIE) are the expert bodies most capable of formulating guidelines for national legislation. Accordingly, Washington has asked the WHO to take the lead in this effort by working with the FAO and the OIE to prepare a report for the experts group.

Since the experts will have only one week in which to discuss biosecurity issues, it is likely that a follow-on negotiation among BWC member states will be required to develop an appropriately detailed set of technical guidelines for the protection, control, and accounting of dangerous pathogens. Recently, a few international organizations have launched initiatives in the biosecurity field. (See International Biosecurity Initiatives Sidebar.) Drawing on the best practices identified by these efforts, BWC member states should establish a technical experts group that would meet on a regular basis to negotiate a set of detailed functional standards that can be implemented through national laws and regulations.

Biosecurity standards would be promulgated and enforced on a national level by existing or newly established governmental entities. To ensure a degree of uniformity and accountability in national implementation, however, it might be necessary to create an international oversight mechanism. One model is provided by the Nuclear Safety Convention, which was adopted in Vienna on June 17, 1994, to establish basic safety guidelines for the location, design, construction, and operation of civilian nuclear power plants.\textsuperscript{14} The Nuclear Safety Convention is an “incentive instrument” in that it does not enforce compliance through formal verification measures but rather through the common interest of the parties in achieving higher levels of nuclear safety. Member states are expected to submit periodic reports on the steps they are taking to implement the agreed guidelines. At regularly scheduled review meetings, each participating country has an opportunity to discuss its own actions and to seek clarification of the reports submitted by others. Political pressure and the need for governments to appear responsible create incentives to join the regime and to comply with the agreed standards.

In much the same way, BWC member states that have voluntarily accepted international standards for the protection, control, and accounting of dangerous pathogens could agree to participate in annual review meetings, which might be organized by a small international secretariat staff. At these meetings, countries would report on the implementation of their national biosecurity regulations and answer questions from other delegations. States that failed to implement or adequately enforce the agreed measures could be subjected to probing questions and political pressure. Participating countries could also exchange information to facilitate implementation of the biosecurity standards. For example, if one country refused to grant a scientist access to select agents because of suspected links to a terrorist organization, the intelligence supporting this decision could be shared with other countries so that they could avoid undercutting one another.

**Recommendations**

Efforts by BWC member states 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. Key issues to be addressed include the following:

*Focus on strengthening the weakest links.*

Highly demanding and expensive standards for laboratory security will be counterproductive if developing countries are technically and financially unable to implement them. Instead, the primary aim of global biosecurity standards should be to strengthen the “weakest links”—those states whose research laboratories and culture collections are so poorly secured that terrorists could penetrate them easily. A realistic goal would be to negotiate a set of minimum performance benchmarks that can be met through a variety of different means, either labor intensive (such as armed guards) or capital intensive (such as electronic surveillance technologies).

*Engage the international scientific community.*

The ultimate success of global biosecurity standards will depend on “buy-in” and voluntary cooperation from microbiologists and laboratory administrators around the world. For this reason,
the regulatory guidelines should not be imposed from the top down but rather developed cooperatively from the bottom up with the active participation of leading scientific organizations, such as the International Union of Microbiological Societies.

**Balance flexibility and uniformity.**

Global biosecurity standards should be flexible enough to be tailored to individual research facilities, yet specific enough to ensure a reasonable degree of consistency and uniformity in their implementation. Overly rigid standards could force universities and other research centers to purchase costly security equipment that is unnecessary or inappropriate to their needs, but standards that are too vague would enable institutions to evade their basic obligations, creating areas of lax implementation that could be exploited by terrorists. Another problem is that regulations tend to be fixed and static, whereas biological science and technology are in constant flux. Thus, a workable system of biosecurity standards must contain a mechanism for periodic review so that the list of regulated agents and the functional guidelines could be revised and updated in response to ongoing advances in scientific knowledge and security measures.

**Encourage compliance by using “carrots” rather than “sticks.”**

The best way to promote international compliance with biosecurity standards is through positive incentives rather than punishments. Creating mechanisms to “incentivize” compliance is generally easier and cheaper than attempting to establish an international policing mechanism. One precedent is the Organization for Economic Cooperation and Development (OECD), which is developing voluntary security guidelines that must be adopted by all states seeking to participate in a planned global network of biological resource centers. The OECD network will effectively create an exclusive “club” whose benefits can be accessed only by meeting the requirements for membership. This arrangement will provide a strong incentive for countries to comply with the agreed biosecurity rules. Similarly, the WHO and other international scientific bodies might make compliance with global biosecurity standards a prerequisite for research grants involving work on dangerous pathogens. **Avoid creating perverse incentives.**

Experts developing global biosecurity standards should try to anticipate their downstream consequences, both positive and negative. Since many scientists have a deep aversion to paperwork, regulations that are too burdensome and costly to implement might simply drive microbiologists and laboratory administrators to circumvent the rules by engaging in informal transfers of pathogens that are not reported to government authorities. It is also essential that biosecurity standards not be so onerous that they deter academic and industrial scientists from pursuing legitimate biomedical or biodefense research on dangerous pathogens or drive research institutions to destroy valuable culture collections in the hope of avoiding regulatory burdens or legal liability. To prevent such negative outcomes, biosecurity procedures should be designed to minimize paperwork and ease compliance. **Integrate national biosecurity regulations with international arms control objectives.**

Ensuring that pathogens are used only for peaceful purposes would help strengthen the legal and ethical norms enshrined in the BWC against the development, production, and stockpiling of biological weapons. At the same time, biosecurity standards, which focus primarily on the threat of bioterrorism, should be linked to efforts to bolster state-level compliance with the convention. For example, biosecurity measures should be designed so that they do not adversely affect the perception of national biodefense programs, which are permitted under the BWC. The line between defensive and offensive work on biological weapons is unavoidably blurry because researchers must use dangerous pathogens to assess threats and to test the effectiveness of defensive systems, such as detectors and protective equipment. Given this inherent ambiguity, excessive security at biodefense laboratories could arouse suspicion that supposedly defensive research activities are being used as a cover for the development of new biological weapons. For this reason, it is essential that countries not invest in biosecurity technologies or procedures that unduly reduce the transparency of biodefense research. At the same time, states should not be forced to reveal critical vulnerabilities that could render the defenses ineffective.
In conclusion, the negotiation of global biosecurity standards would represent a departure from arms control as it has been traditionally practiced. Rather than creating a legally binding treaty that is subject to intrusive verification by an international inspectorate, as in the case of the Chemical Weapons Convention, the biosecurity regime would consist of a set of agreed guidelines implemented through national legislation. To ensure a reasonable degree of uniformity and accountability in implementation, a small international secretariat might be established to provide oversight and to organize annual review meetings. Further, instead of focusing on state-level proliferation of biological weapons, global biosecurity standards would reduce the risk of theft or diversion of dangerous 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.

**U.S. Biosecurity Legislation**

The U.S. Congress first introduced controls on dangerous pathogens after a 1995 incident called attention to the lack of government regulation in this area. Larry Wayne Harris, a licensed microbiologist and neo-Nazi sympathizer in Columbus, Ohio, used a forged letterhead to order three vials of freeze-dried Yersinia pestis (plague) bacteria from American Type Culture Collection. After Harris’ repeated calls to check on the status of his order aroused suspicion, he was arrested and later convicted of one count of mail fraud.

In response to the Harris case, the Senate Judiciary Committee held hearings on how to prevent the unauthorized acquisition of dangerous pathogens by criminals and terrorists. The following year, Congress passed the Anti-Terrorism and Effective Death Penalty Act of 1996, which included a section imposing new controls on facilities that ship or receive dangerous pathogens and toxins. Pursuant to this legislation, federal regulations that went into effect April 15, 1997, required anyone shipping or receiving agents on a list of hazardous microbial pathogens and toxins (termed “select agents”) to register with the U.S. Centers for Disease Control and Prevention (CDC) and file a report on each individual transaction. But the regulations contained a major loophole: laboratories that possessed or worked with listed pathogens or toxins but did not transfer or receive them were not required to register. In the aftermath of the 2001 anthrax letter attacks, the Senate Judiciary Committee held hearings at which FBI officials testified that because of the regulatory loophole, the U.S. government did not have a comprehensive list of facilities or scientists in the United States that possessed or worked with anthrax.

In an effort to close this loophole, Congress included two provisions on select agents in an anti-terrorism bill (the so-called USA PATRIOT Act) signed into law October 26, 2001. Section 817 makes it a crime to knowingly possess any biological agent, toxin, or delivery system that cannot be “reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose.” In addition, Section 175b specifies several categories of “restricted persons” who are prohibited from shipping, receiving, transporting, or possessing select agents. One such category covers nonresident aliens from countries on the State Department’s list of states that support international terrorism. (The list, which is subject to change, includes Cuba, Iran, Libya, North Korea, Sudan, and Syria.)

On June 12, 2002, President George W. Bush signed a second piece of legislation called the Public Health Security and Bioterrorism Preparedness and Response Act. Title II of this act, “Enhanced Controls for Dangerous Biological Agents and Toxins,” requires all entities in the United States that possess, use, or transfer one or more of the 39 pathogens and toxins on the Select Agents List to register with the CDC and implement safety and security measures. In addition, all scientists seeking to work with select agents must undergo an FBI background check. The Bioterrorism Preparedness Act also grants authority to the United States Department of Agriculture’s Animal and Plant Health Inspection Service (APHIS) to develop a separate list of pathogens and toxins that pose a severe threat to animal health or to animal or plant products. The CDC and APHIS coordinate in regulating 16 so-called overlap agents that appear on both the human and animal lists. An estimated 1,469 facilities in the United States that possess, work with, or transfer listed agents are covered by the new rules; clinical laboratories are exempt unless they retain samples of...
pathogens for long periods. Laboratory security plans must be prepared by June 12, 2003, and each registered entity must be in full compliance with the new regulations by November 12, 2003.

The main objective of the biosecurity regulations is to track “who, what, and where”—who has access to listed pathogens and toxins, what agents have been accessed, and where in a facility they are in use. Because of the wide variety of facilities working with listed agents, the guidelines are not highly prescriptive. Instead, each institution is required to conduct threat and vulnerability assessments and develop a comprehensive plan to ensure the security of areas containing listed pathogens and toxins. Once the security plan has been developed, it must be submitted to the CDC or APHIS, performance tested, and updated periodically. Officials from the two federal agencies may also conduct unannounced inspections of declared sites.

International Biosecurity Initiatives

Organization for Economic Cooperation and Development

The Organization for Economic Cooperation and Development (OECD), a group of 30 advanced industrial countries headquartered in Paris, has undertaken the most ambitious international effort to date to regulate dangerous pathogens. The OECD has long been interested in “biological resource centers” (BRCs), defined as government, industry, or academic facilities that house, control, test, or use biological materials. BRCs are a key element of the research infrastructure for the life sciences and the biotechnology industry, but many valuable culture collections are disappearing as governments withdraw financial support. In response to this problem, the OECD is organizing a global network of BRCs that will function as a “virtual lending library” to permit the free exchange of microbial cultures among its members.

In mid-2001, the OECD established a Task Force on BRCs to begin negotiations on the global network. In addition to the 30 members of the OECD, several nonmember countries were invited to participate as nonvoting observers. Establishing the BRC network requires the harmonization of national rules for accreditation, quality control standards for the composition and purity of cultures, and funding arrangements. After the terrorist attacks of September and October 2001, the United States asked that the mandate of the BRC Task Force be expanded to include biosecurity measures.

The current plan is for the OECD Task Force to negotiate a set of regulatory guidelines for the BRC network, which will be presented for approval at a meeting of science ministers from the participating countries, scheduled for January 2004. Given the tight deadline, the task force is unlikely to develop detailed technical security standards but instead broad guidelines, and the final rules will not be legally binding. Nevertheless, because the free exchange of pathogens among facilities within the BRC network will be possible only if all the participating facilities are secure, countries that do not meet the agreed minimum standards of quality, safety, and security will be excluded from the network. To certify and enforce the standards on a national basis, each participating government must select an accrediting agency, which will conduct periodic checks of biosafety and biosecurity measures at the participating BRCs.

Although negotiation of the BRC network currently involves the 30 OECD member states plus roughly a dozen observers, member countries are conducting regional consultations with other states, with a view to creating a global network of BRCs. Eventually, the network might be spun off from the OECD and a small, stand-alone international secretariat established to serve as gatekeeper.

Group of Seven Plus Mexico

In response to the events of the fall of 2001, health ministers from the G-7 countries (Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States) plus Mexico met in
Preventing the Misuse of Pathogens: The Need for Global Biosecurity
Published on Arms Control Association (https://www.armscontrol.org)

Ottawa, Canada, November 7, 2001, to forge a new partnership called the Global Health Security Initiative. Among the stated goals of this partnership is “to improve linkages among laboratories, including level four [Biosafety Level-4] laboratories, in those countries which have them.” Directors of maximum-containment laboratories from participating countries met in Lyons, France, March 12, 2002, to discuss the establishment of a Level 4 Laboratory Network that will develop standard protocols for the transfer of pathogens among BSL-4 facilities.

Australia Group

The United States and 32 other like-minded countries “harmonize” their national export controls on dual-use materials and equipment that could be involved in the production of chemical and biological weapons through an informal coordinating mechanism known as the Australia Group. This body was established in 1985 in response to the widespread use of chemical weapons by Iraq during the Iran-Iraq war. The Australia Group initially developed a “control list” of chemical weapons precursors that were to be denied to countries assessed to be seeking a chemical warfare capability. In 1990, in response to growing concern over the proliferation of biological weapons, the Australia Group added measures to tighten export controls on dangerous pathogens and dual-use biotechnology equipment.

Although the primary aim of the Australia Group has been to impede state-level proliferation, in June 2002 the group placed greater emphasis on bioterrorism by adding eight toxins of possible terrorist interest to its biological control list. One drawback of the Australia Group is that its membership does not include a number of important countries, such as China, Russia, India, Pakistan, and Iran. Several developing countries also oppose the group’s existence on political grounds, claiming that it is discriminatory and unfairly impedes the economic development of targeted states.

Other International Organizations

The Organization for Security and Co-operation in Europe (OSCE) supports proposed standards for licensing and enforcement procedures related to dangerous pathogens and dual-use biotechnology equipment. The World Customs Organization has started sharing information with Interpol and the World Health Organization to combat the smuggling of biological, chemical, and radioactive materials. The International Maritime Organization plans to negotiate an agreement to halt the shipping of biological agents for hostile purposes.

Biotechnology and Pharmaceutical Industry

Although most work with dangerous pathogens takes place in university and government laboratories, elements of the biotechnology and pharmaceutical industries have begun to address biosecurity issues. In 2002 the Swiss pharmaceutical trade association Interpharma developed a draft code of conduct titled “Biosafety and Biosecurity—Industry Best Practices to Prevent Use of Biohazardous Material.” It calls on companies to establish internal regulations and procedures for handling dangerous pathogens, including detailed inventories of materials stored and transferred, transparency in the acquisition of pathogens and toxins from commercial sources and scientific collaborators, security measures to prevent access by unauthorized individuals, safe transport of biohazardous materials, and treatment of wastes to avoid discharging infectious agents into the environment. Return to text.

Table 1. Characteristics of Fissile Materials and Pathogens

<table>
<thead>
<tr>
<th>Fissile Materials</th>
<th>Biological Pathogens</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not exist in nature</td>
<td>Generally found in nature</td>
</tr>
<tr>
<td>Nonliving, synthetic</td>
<td>Living, replicative</td>
</tr>
</tbody>
</table>
Difficult and costly to produce | Easy and cheap to produce
---|---
Not diverse: plutonium and highly enriched uranium are the only fissile materials used in nuclear weapons | Highly diverse: more than 20 pathogens are suitable for biological warfare
Can be inventoried and tracked in a quantitative manner | Because pathogens reproduce, inventory control is unreliable
Can be detected at a distance from the emission of ionizing radiation | Cannot be detected at a distance with available technologies
Weapons-grade fissile materials are stored at a limited number of military nuclear sites. | Pathogens are present in many types of facilities and at multiple locations within a facility
Few nonmilitary applications (such as research reactors, thermo-electric generators, and production of radioisotopes) | Many legitimate applications in biomedical research and the pharmaceutical/biotechnology industry

Table 2. Maximum-Containment (BSL-4) Laboratories Worldwide

<table>
<thead>
<tr>
<th>Country</th>
<th>Name of Laboratory</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>National High Security Quarantine Laboratory</td>
<td>Geelong</td>
</tr>
<tr>
<td>Australia</td>
<td>Victorian Infectious Disease Reference Laboratory</td>
<td>Melbourne</td>
</tr>
<tr>
<td>Belarus</td>
<td>Research Institute for Epidemiology and Microbiology</td>
<td>Minsk</td>
</tr>
<tr>
<td>Brazil</td>
<td>Universidade Estadual Paulista, Campus de Botucatu</td>
<td>Sao Paulo</td>
</tr>
<tr>
<td>Canada</td>
<td>Canadian Science Centre for Human and Animal Health</td>
<td>Winnipeg, Manitoba</td>
</tr>
<tr>
<td>France</td>
<td>Jean Merieux Laboratory</td>
<td>Lyons</td>
</tr>
<tr>
<td>Gabon</td>
<td>International Center for Medical Research</td>
<td>Franceville</td>
</tr>
<tr>
<td>Germany</td>
<td>Bernhard Nocht Institute for Tropical Medicine</td>
<td>Hamburg</td>
</tr>
<tr>
<td>Japan</td>
<td>National Institute of Infectious Diseases</td>
<td>Tokyo</td>
</tr>
<tr>
<td>Russia</td>
<td>Institute for Viral Preparations</td>
<td>Moscow</td>
</tr>
<tr>
<td>Russia</td>
<td>Vector Laboratory</td>
<td>Novosibirsk, Siberia</td>
</tr>
<tr>
<td>Spain</td>
<td>Center for Investigations of Animal Health</td>
<td>Madrid</td>
</tr>
<tr>
<td>South Africa</td>
<td>National Institute of Virology</td>
<td>Johannesburg</td>
</tr>
</tbody>
</table>
NOTES
1. For useful comments on an earlier version of this paper, I am indebted to Gerald L. Epstein of the Defense Threat Reduction Agency, Reynolds M. Salerno and colleagues at Sandia National Laboratories, Janet Shoemaker of the American Society for Microbiology, Frank P. Simione of American Type Culture Collection, and Gregory J. Stewart of the U.S. Department of State.


Jonathan B. Tucker is a senior fellow at the United States Institute of Peace (USIP) on leave from the Center for Nonproliferation Studies at the Monterey Institute of International Studies. USIP will publish a longer version of this article in the fall.

Source URL: https://www.armscontrol.org/act/2003-06/features/preventing-misuse-pathogens-need-global-biosecurity