BIOLOGICAL TERRORISM: LEGAL MEASURES FOR PREVENTING CATASTROPHE

BARRY KELLMAN*

* Professor, DePaul University College of Law; B.A. University of Chicago, 1973; J.D. Yale Law School, 1976. Currently, Professor Kellman is Visiting Scholar at The Center for Nonproliferation Studies, Monterey Institute of International Studies. Gratitude is deeply owed to Michael L. Moodie for reviewing an early draft; to M. Cherif Bassiouni for providing insights relevant to criminal law enforcement; and most especially to Suzanne E. Spaulding for providing the opportunity, in connection with The National Commission on Terrorism, to develop many of the ideas herein.

Biological terrorism is a truly despicable subject, raising nightmares of primal fear. Disease—plague, smallpox, and other decimating maladies—is dire trauma embedded in humanity's collective consciousness. Now, when the threat of thermonuclear holocaust may be ebbing, a few zealots or criminals can kill thousands (or more) and destabilize social order by revealing that no government, even that of superpower America, can protect its citizenry. A biological attack means that everyone is vulnerable. This is terrorism nonpareil.

This Article's agenda is modest: Set forth legal initiatives that might reduce the risks of bioterrorism, recognizing that those initiatives must be combined with nonlegal policies. For example, more money to develop sensors and to train medical personnel could be advantageously spent without proposing or amending legislation or regulations. Legal initiatives should be seen, therefore, as only part of a larger policy response to reduce terrorism opportunities, strengthen detection, focus resources, and deter those terrorists who are averse to harsh

penalties.[1]

The agenda here is also overt. Law's contribution to preventing bioterrorism, though limited, is crucial. And time, unfortunately, is not on the side of the angels. This Article, therefore, is a call to action.

Part I of this Article synthesizes the vast literature on bioterrorism,[2] describing various diseases that could be used and how those diseases might fulfill different objectives. Part II and Part III develop this Article's thesis that threats of bioterrorism call for a two-dimensional set of carefully tailored policies to reduce biological threats, but do not justify radical new overtures. Proposed regulatory modifications can restrict the availability of useful materials and equipment and increase the cost and likelihood of detection. Part II advances a regulatory agenda, mindful to not over-burden the bio-

---

1. *See generally Countering the Changing Threat of International Terrorism*, REPORT OF THE NATIONAL COMMISSION ON TERRORISM (2000), *available at* http://www.fas.org/irp/threat/commission.html.

2. *See generally* MARIE I. CHEVRIER ET AL., BIOLOGICAL WEAPONS PROLIFERATION: REASONS FOR CONCERN, COURSES OF ACTION (Henry L. Stimson Ctr., Report No. 24, Jan. 1998) (containing five chapters on the Biological Weapons Convention by various authors) [hereinafter BIOLOGICAL WEAPONS PROLIFERATION], *available at* http://www.stimson.org/pubs/cwc/index.html; RICHARD A. FALKENRATH ET AL., AMERICA'S ACHILLES' HEEL (1998) (describing America's vulnerability to terrorism involving weapons of mass destruction); Ronald M. Atlas, *Combating the Threat of Biowarfare and Bio-terrorism: Defending Against Biological Weapons is Critical to Global Security*, 49 BIOSCIENCE 465 (1999); Jose Vegar, *Terrorism's New Breed*, BULL. ATOMIC SCIENTISTS, Mar.-Apr. 1998, at 50 (discussing the likelihood that today's terrorists will use chemical and biological weapons), *available at* http://www.bullatomsci.org/issues/1998/ma98/ma98vegar.html; Tom Carter, *Biological Terrorism: A Threat Overlooked*, WASH. TIMES, Jan. 16, 2000, at C1; Leonard A. Cole, *The Specter of Biological Weapons*, SCIENTIFIC AMERICAN, Dec. 1996, at 60, *available at* http://www.sciam.com/1296issue/1296cole.html; Thomas V. Inglesby, *The Germs of War; How Biological Weapons Could Threaten Civilian Populations*, WASH. POST, Dec. 9, 1998, at H1; Zachary Selden, *Biological Weapons: Defense Improves, but the Threat Remains*, BUSINESS EX. FOR NAT'L SEC., http://www.bens.org/pubs/bioup.html (last visited January 5, 2001); Dane Jones, *Biological Warfare and the Implications of Biotechnology*, Dep't of Chemistry & Biochemistry, Calif. Polytech. State Univ., *at* http://www.calpoly.edu/~drjones/biowar-e3.html (last visited January 5, 2001); POTOMAC INST. POLICY STUDIES, PROCEEDINGS REPORT PIPS-98-3, SEMINAR ON EMERGING THREATS OF BIOLOGICAL TERRORISM: RECENT DEVELOPMENTS (1998); Ron Purver, *Chemical and Biological Terrorism: The Threat According to the Open Literature*, Canadian Security Intelligence Service, *at* http://www.csis-scrs.gc.ca/eng/miscdocs/purve.html (June 1995) (reporting on the possible terrorist use of chemical or biological agents); *National Symposium on Medical and Public Health Response to Bioterrorism*, EMERGING INFECTIOUS DISEASES, July-August 1999; JAMES H. ANDERSON, MICROBES AND MASS CASUALTIES: DEFENDING AMERICA AGAINST BIOTERRORISM (1998); BIOLOGICAL WEAPONS: WEAPONS OF THE FUTURE? (Brad Roberts ed., 1993).

pharmaceutical industry, that would raise barriers to obtaining pathogens and weaponization technology. Since these regulatory measures are not perfectly prophylactic (i.e. terrorists might still gain deadly agents), modifications of law enforcement policies should detect, investigate, and stop terrorists who overcome the regulatory barriers and prepare weapons. Part III discusses the unique problems that clandestine biological terrorism presents for law enforcement and recommends measures to better identify bioterrorism threats without overstepping civil liberties and privacy rights.

Put simply, the best strategy is two-pronged: Deny access to biological weapons capabilities, and—if capabilities are obtained—apprehend the terrorist before attack. Legal measures offer no guarantee for preventing bioterrorism, but the measures described here might substantially diminish risks when combined with enhanced pathogen-relevant research and development, improved planning and communication among officials, and advanced intelligence capabilities.

Many topics tangentially relevant to biological terrorism are not discussed here, either because law cannot significantly address them or because, even if addressed, law cannot materially diminish the risks of biological terrorism. This Article will not discuss the broad array of issues that span counter-terrorism policy.[3] Neither will it assess the merits of

3. *See, e.g.*, GAO, GAO/NSIAD-99-135, COMBATING TERRORISM: ISSUES TO BE RESOLVED TO IMPROVE COUNTERTERRORISM OPERATIONS (1999) (detailing the array of government counterterrorist operations); *see generally* HENRY H. HAN, TERRORISM & POLITICAL VIOLENCE: LIMITS AND POSSIBILITIES OF LEGAL CONTROL (1993) (providing a broad discussion of measures to combat state-sponsored terrorism); WALTER LAQUEUR, THE NEW TERRORISM, FANATICISM AND THE ARMS OF MASS DESTRUCTION (1999) (discussing motivations of certain new terrorists); LEGAL RESPONSES TO INTERNATIONAL TERRORISM: U.S. PROCEDURAL ASPECTS (M. Cherif Bassiouni ed., 1998) (analyzing modalities of international criminal law useful in combating terrorism); JOHN F. MURPHY, STATE SUPPORT OF INTERNATIONAL TERRORISM (1989) (discussing the extent of state-sponsored terrorism); GLENN SCHWEITZER & CAROLE C. DORSCH, SUPERTERRORISM (1998) (describing links between organized crime, especially in Russia, and terrorism); JESSICA E. STERN, THE ULTIMATE TERRORISTS (1999) (discussing potential biological weapons and their acquisition, uses, and potential users); Beverly Allen, *Talking "Terrorism": Ideologies and Paradigms in a Postmodern World*, 22 SYRACUSE J. INT'L & COM. 7 (1996); Jacqueline Ann Carberry, Comment, *Terrorism: A Global Phenomenon Mandating a Unified International Response*, 6 IND. J. GLOBAL LEG. STUD. 685 (1999) (advocating multilateral terrorism convention); Joseph Dellapenna, *Legal Remedies for Terrorist Acts*, 22 SYRACUSE J. INT'L L. & COM. 13 (1996); Yassin El-Ayouty, *International Terrorism Under the Law*, 5 ILSA J. INT'L & COMP. L. 485 (1999) (discussing terrorism under Islamic and international law); Barry Kellman, *Catastrophic Terrorism—Thinking Fearfully, Acting Legally*, 20 MICH. J. INT'L L. 537

promoting enhanced research on pathogenicity nor consider the appropriate levels of stockpiled vaccines; these questions are better addressed by the medical and pharmaceutical communities.[4] This Article will not discuss the need for enhanced foreign intelligence; crucial information is not publicly available, and legal measures would not make much difference.[5] Nor will this article address preparations to

---

(1999) (discussing private, federal, and international measures to combat terrorism); Neil C. Livingstone, *Terrorism: Conspiracy, Myth and Reality*, 22 FLETCHER F. WORLD AFF. 1 (1998) (questioning extent of terrorist threat); John-Alex Romano, Note, *Combating Terrorism and Weapons of Mass Destruction: Reviving the Doctrine of a State of Necessity*, 87 GEO. L.J. 1023 (1999) (discussing application of laws of war to international terrorism); Yonah Alexander, *Terrorism: Threats and Responses*, WORLD & I, June 1999, at 80 (highlighting trends in government-sponsored terrorism); John F. Sopko, *The Changing Proliferation Threat*, FOREIGN POL'Y, Dec. 1996, at 3 (describing increase of non-ideological terrorism); *Terrorist Threats to the United States: Hearing Before the Special Oversight Panel on Terrorism of the House Comm. on Armed Services*, 106th Cong. (2000); BRAD ROBERTS, HYPE OR REALITY: THE "NEW TERRORISM" AND MASS CASUALTY ATTACKS (Chemical and Biological Arms Control Institute 2000).

4. *See* COMM. ON R&D NEEDS FOR IMPROVING CIVILIAN MEDICAL RESPONSE TO CHEMICAL AND BIOLOGICAL TERRORISM INCIDENTS, INST. OF MEDICINE AND BD. ON ENVT'L STUDIES & TOXICOLOGY, COMM'N ON LIFE SCIENCES, NAT'L RES. COUNCIL, CHEMICAL AND BIOLOGICAL TERRORISM: RESEARCH AND DEVELOPMENT TO IMPROVE CIVILIAN MEDICAL RESPONSE ch. 8 (1999), *available at* http://stills.nap.edu/html/terrorism/ch8.html (discussing the availability, safety, and efficacy of drugs and other therapies) [hereinafter COMM. ON R&D NEEDS]; *see also* Jaclyn Shoshana Levine, *The National Vaccine Injury Compensation Program: Can It Still Protect an Essential Technology*, 4 B.U. J. SCI. & TECH. 9 (1998); David C. Mowery & Violaine Mitchell, *Improving the Reliability of the U.S. Vaccine Supply: An Evaluation of Alternatives*, 20 J. HEALTH POL., POL'Y & L. 973 (1995) (discussing the reliability of U.S. vaccine supplies); Phillip K. Russell, *Development of Vaccines to Meet Public Health Needs: Incentives and Obstacles*, 7 RISK: HEALTH SAFETY & ENV'T 239 (1996) (discussing how politics, lack of a delivery plan, and regulatory costs interfere with global provision of vaccines); Jeff Nesmith, *Target America: Biochemical Warfare—Public Health Sector Ill-equipped for Battle; Poor Funding for Equipment and Training Could Cost Lives in the Event of Bio-terrorism*, ATLANTA J. & CONST., Aug. 2, 1998, at 2E; MICHAEL E. STOUT, COMBATING BIOLOGICAL TERRORISM: IS DEPARTMENT OF DEFENSE PREPARED TO SUPPORT U.S. GOVERNMENT INTERAGENCY QUARANTINE OPERATIONS? (U.S. Army War College 2000) (analyzing military readiness for medical emergencies); MARY J.R. GILCHRIST, LABORATORY SAFETY, MANAGEMENT, AND DIAGNOSIS OF BIOLOGICAL AGENTS ASSOCIATED WITH BIOTERRORISM (American Society for Microbiology 2000) (recommending training epidemiologists to recognize unusual pathogens); Scott Lillibridge, *A Public Health Response to Bioterrorism*, 6 MEDICINE & GLOBAL SURVIVAL 82 (2000) (recommending that the Surgeon General have federal leadership for bioterrorism response); SENATE COMM. ON HEALTH, EDUC., LABOR & PENSIONS, PUBLIC HEALTH THREATS AND EMERGENCIES ACT: REPORT TO ACCOMPANY S. 2731 (2000); Victoria V. Sutton, *A Precious "Hot Zone"—The President's Plan to Combat Bioterrorism*, 164 MIL. L. REV. 135 (2000).

5. *See generally* HOUSE PERMANENT SELECT COMM. ON INTELLIGENCE, 104TH CONG., IC21: INTELLIGENCE COMMUNITY IN THE 21ST CENTURY ch. XIII (1996) (describing intelligence and law enforcement operations); Russell J. Bruemmer, *Intelligence Community Reorganization: Declining the Invitation to Struggle*, 101 YALE L.J. 867 (1992) (discussing intelligence needs); Jonathan M. Fredman, *Intelligence*

respond after an attack happens; those measures are necessary but do not serve to prevent the attack.[6]

A vast set of issues, substantially outside the scope of this Article and meriting separate attention, concerns the international proliferation of biological weapons and negotiated efforts to stanch their spread.[7] Russia had an active biological weapons research program into the early 1990s; many experts believe that the Russian military actively pursued a biological weapons program thereafter and may still be doing so.[8] Even if Russia is not actively pursuing biological weapons capabilities, there is the risk that its facilities are leaking equipment and perhaps even pathogens to other States or terrorist groups.[9] Iraq's biological weapons program was uncovered by United Nations inspectors in 1995.[10] Many

---

Agencies, Law Enforcement, and the Prosecution Team, 16 YALE L. & POL'Y REV. 331 (1998) (same).

6. Most post-attack efforts will be conducted under the authority of the Stafford Act, 42 U.S.C. § 5121 *et seq.* (2000). For the most thorough and current discussion of response capabilities, see ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION, FIRST ANNUAL REPORT TO THE PRESIDENT AND THE CONGRESS, *Part I: Assessing the Threat*, *available at* http://www.infowar.com/class_3/00/class3_tp-terr.shtml (Dec. 15, 1999); AMY E. SMITHSON & LESLIE-ANNE LEVY, ATAXIA: THE CHEMICAL AND BIOLOGICAL TERRORISM THREAT AND THE U.S. RESPONSE (Henry L. Stimson Ctr., Report No. 35, Oct. 2000), *available at* http://www.stimson.org/pubs/allpubs.htm; PETER E. BARTH, COUNTERING THE BIOLOGICAL WEAPONS THREAT TO THE HOMELAND (U.S. Army War College 2000).

7. *See generally Measures to Eliminate International Terrorism: Report of the Working Group*, G.A. Res. 110, U.N. GAOR, 54th Sess. (1999), *available at* http://www.un.org/documents/ga/res/54/a45r110.pdf; Jonathan B. Tucker & Kathleen M. Vogel, *Preventing the Proliferation of Chemical and Biological Weapon Materials and Know-How*, NONPROLIFERATION REV., Spring 2000, at 88; BRAD ROBERTS & MICHAEL MOODIE, COMBATING NBC TERRORISM: AN AGENDA FOR ENHANCING INTERNATIONAL COOPERATION (Chemical and Biological Arms Control Institute 2000).

8. *See* Atlas, *supra* note 2, at 465; Federation of American Scientists, *Is Russia Prepared for Offensive Biological War?*, *at* http://209.207.236.112/nuke/guide/russia/facility/cbw/ucs980411.htm (April 11, 1998); *see also* Jones, *supra* note 2; GULBARSHYN BOZHEYEVA ET AL., FORMER SOVIET BIOLOGICAL WEAPONS FACILITIES IN KAZAKHSTAN: PAST, PRESENT, AND FUTURE, (Ctr. Nonproliferation Studies, Monterey Inst. Int'l Studies, Occasional Paper No. 1, 1999); C.J. Davis, *Nuclear Blindness: An Overview of the Biological Weapons Programs of the Former Soviet Union and Iraq*, 5 EMERGING INFECTIOUS DISEASES 509 (1999).

9. *See* AMY E. SMITHSON, TOXIC ARCHIPELAGO: PREVENTING PROLIFERATION FROM THE FORMER SOVIET CHEMICAL AND BIOLOGICAL WEAPONS COMPLEXES 19 (Henry L. Stimson Ctr., Report No. 32, December 1999), *available at* http://www.stimson.org/pubs/projpubs.htm.

10. *See id.* Iraqi officials admitted producing anthrax, botulinum toxin, and aflatoxin after years of claiming that they conducted only defensive research. They also admitted preparing—but not using—biological weapons-filled munitions, including twenty-five Scud missile warheads, aerial bombs, and aerial dispensers

experts believe that Iran has a military biological program even if it does not now have an offensive weapons capability.[11] Other countries currently suspected of having programs include: China, Taiwan, North Korea, Syria, Egypt, Cuba, Israel, former Soviet States, the United States, and Japan.[12] According to recently-substantiated allegations, a 500-liter medical fermentation device was sent from the United States to a pharmaceutical plant in China suspected of manufacturing chemical and biological agents for military purposes.[13] Lastly international treaty negotiations are proceeding actively for a new protocol to the Biological Weapons Convention,[14] but that protocol does not explicitly confront threats of terrorism.[15]

---

during the Gulf War. UNSCOM destroyed a range of biological weapons production equipment, seed stocks, and growth media, which Iraq claimed was for use in its biological weapons programs. UNSCOM believed Iraq greatly understated its biological agent production and could have been holding back agents that are easily concealed. Iraq resisted dismantling the Al Hakam biological weapons production facility for nearly one year, claiming that it was a legitimate civilian facility designed to produce single proteins and biopesticides. After discovering in 1995 that Iraq manufactured over 500,000 liters of biological weapons agents at the facility between 1989-90, UNSCOM pressed Iraq to destroy Al Hakam in the summer of 1996. *See* Iraq Weapons of Mass Destruction Programs, U.S. Gov't White Paper (Feb. 13, 1998), *available at* http://www.state.gov/www/regions/nea/iraq_white_paper.html. Iraq has the expertise to quickly resume a small-scale biological weapons program using facilities currently producing vaccines and other pharmaceuticals. Without effective monitoring, Iraq could probably begin production within a few days. For example, Iraq could convert production of biopesticides to anthrax simply by changing seed material. *See* Gregory Koblenz, *Countering Dual-Use Facilities: Lessons from Iraq and Sudan*, JANE'S INTELL. REV., Mar. 1, 1999, at 48; Judith Miller & William J. Broad, *Iraq's Deadliest Arms: Puzzles Breed Fears*, N.Y. TIMES, Feb. 26, 1998, at A1.

11. *Biological Warfare: The Poor Man's Atomic Bomb—Iran*, JANE'S INTELL. REV., Mar. 1, 1999, at 44; Judith Miller & William J. Broad, *Bioweapons in Mind, Iranians Lure Needy Ex-Soviet Scientists*, N.Y. TIMES, Dec. 8, 1998, at A1.

12. *See* William S. Cohen, *Preparing for a Grave New World*, WASH. POST, July 26, 1999, at A19; Cole, *supra* note 2, at 62.

13. *See* Douglas Burton, *Trie's Deadly Deals*, INSIGHT ON THE NEWS, Mar. 20, 2000, at 14.

14. For the text and a discussion of the subsequent development of the 1972 Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on Their Destruction, see http://dosfan.lib.uic.edu/treaties/bwc1.htm (last visited Jan 5, 2001).

15. *See* Amy E. Smithson, *Man Versus Microbe: The Negotiations to Strengthen the BWC*, *in* BIOLOGICAL WEAPONS PROLIFERATION, *supra* note 2, at 107; Jonathon B. Tucker, *Verification Provisions of the Chemical Weapons Convention and Their Relevance to the Biological Weapons Convention*, *in* BIOLOGICAL WEAPONS PROLIFERATION, *supra* note 2, at 77; Gilliam R. Woollett, *Industry's Role, Concerns, & Interests in the Negotiation of a BWC Compliance Protocol*, *in* BIOLOGICAL WEAPONS PROLIFERATION, *supra* note 2, at 39; Scott Keefer, *International Control of Biological Weapons*, 6 ILSA J. INT'L & COMP. L. 107, 131-38 (1999) (discussing the protocol to the Biological Weapons Convention of 1972); Kyle B. Olson, *Aum Shinrikyo: Once*

I. UNDERSTANDING BIO-TERRORISM

Because a catastrophic bioterrorism attack has not yet happened, trying to understand the phenomenon entails some speculation based on reasonable extrapolations both from the scientific understanding of pathogens and from the social science understanding of terrorist behavior. There has been only one notable effort to develop and employ biological capabilities for terrorist purposes, which was by the Japanese cult Aum Shinrikyo.

Aum devoted vast sums of money, time, and considerable expertise to the task of making biological weapons, but it was not successful. Before puncturing bags of sarin nerve gas on Tokyo subway trains on March 20, 1995, killing twelve people and injuring more than 5,000, the cult had sought to acquire a wide range of weapons, including biological weapons. In April 1990, Aum attempted to attack the Japanese parliament with botulinum toxin aerosol.[16] In 1992, Aum sent a mission to Zaire to assist in the treatment of Ebola victims in order to find a sample of the Ebola strain to take back to Japan for culturing purposes. In June 1993, the cult tried to release poison at the wedding of the crown prince. Later that month, Aum attempted to spray anthrax spores from the roof of a building in Tokyo.[17] All these attacks were unsuccessful and resulted in no casualties. The consequences might have been drastically different had the weapons been properly disseminated.[18]

The cult built weapons under the guidance of well-trained biologists and chemists. They created a sophisticated biological research facility without attracting the attention of the Japanese or other governments. When Japanese officials investigated Aum's compound after the 1995 attack, they found large amounts of equipment indispensable to cultivating bacteria

---

and Future Threat?, 5 EMERGING INFECTIOUS DISEASES 513 (1999).

16. According to at least one leading expert, Aum never succeeded in developing a toxic strain of botulinum toxin. *See* W. Seth Carus, *Biohazard*, NEW REPUBLIC, Aug. 2, 1999, at 15.

17. *See* STAFF OF SENATE GOV'T AFFAIRS PERMANENT SUBCOMM. ON INVESTIGATIONS, 104TH CONG., GLOBAL PROLIFERATION OF WEAPONS OF MASS DESTRUCTION: A CASE STUDY ON THE AUM SHINRIKYO (1995), *available at* http://www.fas.org/irp/congress/1995_rpt/aum/part01.htm.

18. *See* FALKENRATH ET AL., *supra* note 2, at 21-23; *see also* Graham S. Pearson, *The Threat of Deliberate Disease in the 21st Century*, *in* BIOLOGICAL WEAPONS PROLIFERATION, *supra* note 2, at 11; Laura Neergaard, *Bio-terrorism*, Infowar.com, *at* http://www.infowar.com/class_3/99/class3_021799b_j.shtml (Feb. 17, 1999).

and viruses, peptone (a substance used to cultivate bacteria), and books and materials on the production of botulism, cholera, and dysentery. At Aum's site in Naganohara, officials found a four-story concrete facility equipped with a "clean room" with specialized ventilation systems and a sealed room to protect cultivated bacteria from leaking. In connection with these operations, Aum produced illegal drugs for their own use and for sale to others.[19]

In January 1995, an Oregon company sold Aum molecular modeling software that simulates molecular experimentation without the need for actual laboratory experimentation. This software is covered by export restrictions to countries such as China but not to Japan. Aum could have used this software to test theoretical designs for toxins. In March 1995, Aum supporters contacted a Missouri company that produces computer software for use in designing new therapeutic drugs but that can also be used to research and develop biological toxins. Although it harbored suspicions, the Missouri company installed software on a computer provided by Aum.[20] Five days before the Tokyo gas attack, authorities discovered three attaché cases containing a small tank to hold liquid, a small motorized fan, a vent, and a battery. The cult had at least two radio controlled drone aircraft, and they were seeking hundreds of small fans as well as thousands of small serum bottles.[21]

The Aum Shinrikyo experience raises several questions addressed in the remainder of this Part. First, why would a terrorist use biological weapons? Second, what pathogens could or would likely be used? And third, could an attack be concocted?

A. Why Attack with Biological Weapons?

Why would anyone use disease to cause mass death? How difficult is it to use biological agents as weapons, assuming the motivation to do so? If biological weapons are used, what

19. *See Global Proliferation of Weapons of Mass Destruction: Hearing Before the Permanent Subcomm. on Investigations of the Senate Gov't Affairs Committee*, 104th Cong. (1995) (statement of John F. Sopko, Deputy Chief Counsel to the Minority), *available at* http://www.fas.org/irp/congress/1995_rpt/aum/part01.htm.

20. *See id.*

21. *See id.*

casualties can be reasonably expected?

Biological weapons have three advantages from a terrorist's perspective. First, they (as well as chemical weapons) offer an optimal death to cost ratio. Second, they are virtually undetectable and can be handled with relative ease by properly trained and inoculated persons. Third, they offer the potential for mass panic that may uniquely serve a terrorist's purposes.

1. Inflicting Casualties

If a terrorist wants to kill thousands of people, biological weapons merit serious consideration. A nuclear weapon, by comparison, can certainly create far more devastation, but making a nuclear weapon is far more difficult and expensive, and smuggling it poses a far greater risk of detection.[22] At the other end of the weapons spectrum, firearms are inexpensive and readily available, but they have the capacity to kill only a few dozen people before being stopped. Explosives present more technical obstacles than firearms, but offer the potential for inflicting far greater casualties. The failed attempt to blow up the World Trade Center building and kill thousands illustrates the difficulties inherent in this tradeoff.[23] The calculus of terrorism, therefore, leads inexorably to biological and chemical weapons. Comparatively, while chemical weapons are easier to make and use, biological weapons are less detectable, less dangerous to the terrorist, and—except in a few scenarios—have greater killing capability.

Estimates vary widely as to the numbers of dead and sick from a bioterrorist attack. Projected seven-figure casualty estimates, based on multiplying the quantity of pathogen necessary to kill an individual, are flawed. Under this methodology, for example, a lethal dose of Type-A botulina toxin can be prepared in concentrations of ten billion micro-organisms per gram; accordingly, eight ounces is enough to kill every living creature on Earth. This arithmetic misleadingly assumes that these doses will be equally and effectively

22. For a discussion of the difficulty of manufacturing and transporting nuclear weapons, see Barry Kellman & David S. Gualtieri, *Barricading the Nuclear Window—A Legal Regime to Curtail Nuclear Smuggling*, 1996 U. ILL. L. REV. 667 (1996).

23. *See* Dov Waxman, *Terrorism: The War of the Future*, 23 FLETCHER F. WORLD AFF. 201, 203 (1999).

disseminated. But most pathogens disseminated among a large population would not be ingested at all and would die harmlessly from natural causes. The pathogens that are ingested would tend to be concentrated in a fraction of that population, and even some of these persons would, for various reasons, not get sick.

Nonetheless, there are reasonable scenarios involving dissemination of pathogens in confined spaces that predict over ten thousand casualties; in extraordinary circumstances, casualties in excess of 100,000 are not fanciful.[24]

2. *Non-Detectability and Manageability*

Besides their capability to cause mass casualties, there are other good reasons (from a terrorist's perspective) to use biological weapons. Pathogens are undetectable or nearly so. Lethal pathogens may be attractive to foreign terrorist organizations or even rogue States seeking to cause catastrophic injury to the United States without exposing themselves to reprisal. Pathogens can be brought into the country by a single individual and can be smuggled through airports or customs checks. Once here, they can be propagated into enormous quantities. Even their use is initially undetectable. An epidemic can be initiated, and it may be days before symptoms are manifest; even then, the attack may be mistaken for a natural outbreak.[25] Terrorists could easily have sufficient time to flee the scene of the attack, and perhaps the jurisdiction altogether, before law enforcement officials learn that a crime has been committed. The time-lag between release and effect on humans thus reduces the risks of a perpetrator being apprehended.[26] Another contribution to anonymity is

24. It would be irresponsible to describe these scenarios here. Admittedly, sophisticated information on how to commit a bioterrorist attack is widely available, and a potential terrorist is unlikely to seek useful information from a law review article. Nevertheless, my information—while not unique or classified—required considerable time and effort to work through potential obstacles. I cannot abide the thought, however remote, that printing this information might contribute to a terrorist enterprise. My preference, therefore, is to ask the reader's indulgence to accept the statement without proof.

25. Because of the possibility of confusing natural outbreaks and bioterrorist attacks, the World Health Organization is initiating responses to calls that it strengthen its disease monitoring capabilities. *See* Debora MacKenzie, *Under Surveillance*, NEW SCIENTIST, Apr. 8, 2000, at 16-17.

26. *See* Purver, *supra* note 2.

that dissemination of pathogens need not leave identifying markers that could be traced back to the perpetrators. No other weapon offers a comparable capability to inflict catastrophic disruption anonymously.

Despite their disease-causing capabilities, some pathogens can be produced and handled safely by persons who are properly equipped, knowledgeable of the risks, and perhaps inoculated against the disease.[27] Starting with a small seed culture, terrorists could easily generate a stockpile and can work with it, carry it, and distribute it without undue risk. Some, but not all, pathogens have the ability to reproduce in the target population. If sufficiently contagious, an attack would only have to be against a small group (perhaps at an airport) who would then do the terrorists' work for them by carrying it out to a wider population. No other weapon offers similar capabilities to spread itself. Therefore, the problems of dissemination (discussed below) can be overcome to some degree by creating a more potent agent.

3. Panic Potential

Arguably the greatest advantage of biological weapons is their ability to cause mass panic. Bombing a large and heavily populated building is terrifying, as is releasing chemical weapons in a confined space such as a subway, but these attacks are geographically limited. A biological attack makes everyone vulnerable, and this insecurity is the terrorists' primary motivation. Moreover, even if not empirically justifiable, humanity fears disease not only for its ability to kill but for the horrifying way in which it kills. While we have no experience with a catastrophic terrorist attack, memories of past epidemics incite fears of future outbreaks. Thus, even if a biological attack kills only a relatively small number, it is likely to generate panic. This shredding of the fabric of the community and exposure of society's vulnerability, perhaps on a global scale, is the incentive for committing such heinous crimes.

Pathogens may appeal to domestic terrorists who have an

27. *See id.* ("[T]he smaller quantities of agent needed on account of their lethality help reduce the costs and complexity of their production or other acquisition, in turn eliminating the necessity for a large infrastructure of personnel and facilities.").

anarchic or mystical sense that the modern era is corrupt, excessively regimented, or materialistic. For those with a profound sense of alienation or those motivated by a distorted sense of religious faith, disease has a unique Biblical history suggesting that God has often inflicted a scourge on the sinful. Inflating the death toll may be seen as performing a sacramental act, manifesting divine retribution that morally justifies mass murder.

B. What Pathogens Might Be Used?

The Centers for Disease Control (CDC) lists thirty-six pathogenic agents, including seven bacteria, thirteen viruses, three rickettsiae, one fungus, and twelve toxins.[28] Bio-engineered variations of these agents, or development of new agents altogether, could expand this list.[29]

1. Likely Pathogens

This Section briefly describes the agents most often cited as potentially weaponizeable and briefly explains their relevant characteristics.[30] It must be noted that no agent is perfect; a terrorist must therefore choose among various characteristics, including:

---

28. *See* 42 C.F.R. § 72, Appendix A (2000).

29. *See The Worldwide Biological Warfare Threat: Testimony Before the House Permanent Select Committee on Intelligence*, 106th Cong. (1999) (statement of John Lauder, Special Assistant to the DCI for Nonproliferation) ("Rapid advances in biotechnology present the prospect of a whole new array of toxins or live agents that will require new detection methods and preventive measures, including vaccines and therapies.") [hereinafter *Worldwide Biological Warfare Threat*], *available at* http://www.cia.gov/cia/public_affairs/speeches/archives/1999/lauder_speech_030399.html. *But see* BAREND TER HAAR, THE FUTURE OF BIOLOGICAL WEAPONS 55-56 (1991) (arguing that "research will bring diseases increasingly under control," and "less improbable than the development of new biological agents might be attempts to improve upon the effectiveness of existing agents" by enhancing resistance to degradation, complicating detection and diagnosis, or speeding infection); Donald L. Louria, *Monstrous Microbes: What the Experts Say*, FUTURIST, Oct. 1981, at 18 ("Any terrorists or people conducting biological warfare who knew what they were doing would not use genetic engineering. There are much deadlier things they can use. . . .") (quoting Herman Lewis, head of recombinant-DNA activities for the National Science Foundation); U.S. OFFICE TECH. ASSESSMENT, THE TERRORIST THREAT 39 (1991) (providing a comprehensive, though now somewhat dated, discussion of the likelihood of a terrorist attack in the United States).

30. *See generally* U.S. Army Inst. Infectious Diseases, Biological Agent Information Papers, *at* http://www.nbc-med.org/SiteContent/MedRef/OnlineRef/GovDocs/BioAgents.html (last visited January 5, 2001) (listing information about relevant pathogens).

- *Pathogenicity of the agent (how likely the agent is to kill its victim)*: Agents can be chosen to sicken, incapacitate, or kill; to spread from person to person or to affect only those initially exposed; and to be susceptible or resistant to medical treatment.
- *Degree to which the agent is contagious or infectious*: The infectiousness of the agent is directly correlated with the mode of weaponization. If the terrorist intends to spray dust an area and infect via an aerosol cloud, then the likelihood of successful delivery is less than direct injection. Therefore, a more infectious agent would be more desirable.
- *Process of contagion and resistance to protective measures or cures*: The terrorist will also choose an agent that is known to be transferable or containable, depending once again on the terrorist's targeted group. For instance, if the intent is to cause a widespread outbreak, an agent that can be transmitted by coughing or contact with others would be more favorable than one that cannot be transmitted by human to human contact. Further, agents have variable lengths of incubation periods, some allowing ample time for vaccination once an outbreak has been identified. Also, agents differ in the length of time between the onset of symptoms and death.
- *Degree of lethality (how many people are likely to be affected)*: In choosing the appropriate agent to execute the mission, the terrorist likely would consider the lethality of the agent. For instance, agents differ in incubation stages, some acting on their hosts quickly and others not showing signs for several days. Moreover, agents differ in their contagion capabilities. Therefore, when the intent is to indiscriminately pass the illness to a large number of people over a period of time, a less lethal but highly infectious agent may be chosen.
- *Potential risk to the terrorist himself*: The terrorist, through his knowledge of the agents and their production methods, may consider the risks of handling that the agent poses to his health in all the steps until it is disseminated. Those whose scientific proficiency bolsters their confidence in handling pathogenic agents may be more willing to weaponize highly pathogenic agents as

compared to those who are wary of the unknown.[31] It may be very important that there is an available vaccine with which the terrorist may vaccinate himself.[32]

a. Smallpox

The smallpox virus is among the most dangerous organisms that might be used by bioterrorists.[33] It is virulently contagious, often fatal, and spread through inhalation.[34] Smallpox was responsible for hundreds of millions of fatalities before widespread vaccinations were thought to have eradicated it. In 1986, the Executive Committee on Orthopox of the World Health Organization unanimously decided to destroy the last strains of smallpox left in the world except for two samples in Moscow and Atlanta.[35] However, unsubstantiated but highly disturbing reports from Russia suggest new concerns.[36] This is

---

31. *See* Cole, *supra* note 2, at 64.

32. *See id.* at 61 ("After all, one can cultivate trillions of bacteria at relatively little risk to one's self with gear no more sophisticated than a beer fermenter and a protein-based culture, a gas mask and a plastic overgarment.").

33. *See* Tara O'Toole, *Smallpox: An Attack Scenario*, 5 EMERGING INFECTIOUS DISEASES 540, 540 (1999), *available at* http://www.cdc.gov/ncidod/EID/vol5no4/otoole.htm; *see also* D.A. Henderson, *Smallpox: Clinical and Epidemiologic Features*, 5 EMERGING INFECTIOUS DISEASES 536, 538 (1999), *available at* http://www.cdc.gov/ncidod/EID/vol5no4/henderson.htm. *See generally* Jason Bardi, *Aftermath of a Hypothetical Smallpox Disaster*, 5 EMERGING INFECTIOUS DISEASES 547 (1999) (describing a step-by-step account of a hypothetical smallpox epidemic), *available at* http://www.cdc.gov/ ncidod/EID/vol5no4/bardi.htm.

34. *See* Henderson, *supra* note 33, at 537. Henderson describes the progression of smallpox infection:

> To sustain itself, the virus must pass from person to person in a continuing chain of infection and is spread by inhalation of air droplets or aerosols. Twelve to 14 days after infection, the patient typically becomes febrile and has severe aching pains and prostration. Some 2 to 3 days later, a popular rash develops over the face and spreads to the extremities. . . . Gradually, scabs form, which eventually separate, leaving pitted scars. Death usually occurs during the second week. . . . In 5% to 10% of smallpox patients . . . [die] within 5 to 7 days.

Id.

35. *See* D.A. Henderson, *Deliberations Regarding the Destruction of Smallpox Virus: A Historical Review, 1980-1998*, Center for Civilian BioDefense Studies, Comm. of the Inst. of Medicine on Smallpox Destruction, *at* http://www.hopkins-biodefense.org/pages/news/destruction.html (Nov. 20, 1998).

36. *See* Charles Siebert, *Smallpox Is Dead: Long Live Smallpox*, N.Y. TIMES MAG., Aug. 21, 1994, at 32. Since 1992, intelligence reports have revealed that stocks of smallpox exist in several places in Russia. *See* Judith Miller, *Poison Island: At Bleak Asian Site, Killer Germs Survive*, N.Y. TIMES, June 2, 1999, at A1. By 1993, rumors surfaced of smallpox in the hands of North Korean bioweapons researchers. *See* William J. Broad & Judith Miller, *Government Report Says 3 Nations Hide Stocks of Smallpox*, N.Y. TIMES, June 13, 1999, at A1; Wendy Orent, *The Smallpox Wars, Biowarfare v. Public Health*, AMERICAN PROSPECT, May-June 1999, at 49; *see*

especially frightening because health authorities, believing the disease to have been virtually eradicated, have discontinued vaccination programs, leaving current populations highly vulnerable to a terrorist attack using smallpox.

b. Anthrax[37]

Anthrax (*Bacillus anthracis*) is often mentioned as the biological agent of choice. Anthrax is a spore that, if inhaled even in extremely low quantities, is nearly always fatal unless the patient is quickly given huge quantities of antibiotics.[38] Ingestion leads to fatigue, coughing, fever, and chest pains; death comes within twenty-four to thirty-six hours.[39] Anthrax has important virtues from a terrorist perspective. It occurs naturally in the soil. Herbivorous animals such as sheep or goats ingest spores while grazing. Seed cultures of the spores can be taken from samples of the wool or skin; taking more samples increases the likelihood of success.[40] Only small samples would be needed, perhaps no larger than a postage stamp. Although anthrax is more common among Caribbean and Eastern Mediterranean countries, it is not impossible to find infected animals in the United States.[41] As a weapon, the primary virtue of anthrax is its lethality; some experts assert that as little as a single gram, efficiently distributed, could kill more than one-third of the United States population.[42] Another advantage is that it is an endospore and thus highly resistant to humidity, pressure, or temperature. Moreover, anthrax can be

---

generally WILLIAM PATRICK ET AL., THE BACTERIAL AND VIRAL TERRORIST THREAT (Potomac Inst. Policy Studies, 1998) (noting that people with smallpox become contagious even during the incubation period); Wendy Orent, *Killer Pox in the Congo*, DISCOVER, Oct. 1, 1999, at 74 (discussing monkeypox outbreak and the retention of smallpox samples for research).

37. For information on anthrax, see Div. of Bacterial & Mycotic Diseases, Centers for Disease Control & Prevention, Disease Information, *at* http://www.cdc.gov/ncidod/dbmd/diseaseinfo/anthrax_g.html.

38. *See* US. Army Inst. for Infectious Diseases, *supra* note 30.

39. *See id.*

40. *See Biological Warfare Defense Information Sheet*, U.S. Navy Manual on Operational Medicine & Fleet Support, http://www.emergency.com/anthrax2.htm (last visited January 5, 2001) ("The disease Anthrax is caused by the bacteria Bacillus anthracis. Anthrax is normally found in sheep, cattle and horses but can be transmitted to humans. . . . Usually humans acquire the disease by skin contact with the bacteria or by inhaling the bacterial spores found in sheep wool.").

41. *See* Div. of Bacterial & Mycotic Diseases, *supra* note 37.

42. *See* Purver, *supra* note 2.

easily propagated. For these and perhaps other reasons, anthrax has been by far the most often pathogen allegedly used in the United States, although most if not all of these alleged uses were hoaxes.[43]

Anthrax, however, has various disadvantages as a weapon. The fact that it is a spore and hence large relative to other agents means that it is difficult to aerosolize for weapons purposes, and, once released, falls rapidly to the ground, thereby diminishing the opportunity for inhalation. Furthermore, anthrax is not contagious except by direct contact. To kill many people would therefore require widespread dissemination. There is a licensed vaccine which, although the subject of considerable controversy in connection with its use during the Gulf War,[44] can be effective if administered soon after exposure. This vaccine would, of course, enable a potential terrorist to handle anthrax without risk of infecting himself.

c. The Plague

Plague (Yersinia pestis) is a contagious bacterium. Only slightly less lethal than anthrax,[45] it is also naturally available and can be scraped from dead animals. In North America, plague is found in certain animals and in their fleas from the Pacific Coast to the Great Plains, and from southwestern Canada to Mexico.[46] It is more difficult to grow than anthrax, requiring a blood agar, but not so difficult as to preclude its potential weaponization. A licensed vaccine that would allow a terrorist to protect himself is available. However, this vaccine is

---

43. *See* Leonard A. Cole, *Anthrax Hoaxes: Hot New Hobby*, BULL. ATOM. SCIENTISTS, July-Aug. 1999, at 7.

44. *See* U.S. Dep't of Defense, Anthrax Vaccination Program, *at* http://www.anthrax.osd.mil (last visited January 5, 2001).

45. Plague is a flea-borne disease transferred from infected rodents to humans. Plague may also be transmitted via aerosol and by inhalation of droplets between coughing patients. It is lethal within a few days of infection unless treated early with antibiotics. Plague resulting from the bite of an infected flea would result in a primary pneumonic form, which in the absence of therapy, would progress to death within a few days. The person exposed would begin to experience fever, chills, headaches, dyspnea, and toxemia within three days. Then, if untreated, the respiratory system would fail and the circulatory system would collapse, leading to death. *See* U.S. Army Inst. for Infectious Diseases, *supra* note 30.

46. Most human cases in the U.S. occur in 2 regions: the region covering northern New Mexico, northern Arizona, and southern Colorado; and the region covering California, southern Oregon, and far western Nevada. *See id.*

used in animal experiments and will provide no protection against the aerosol exposure; a terrorist who chooses an aerosol route of dissemination would have to immediately take the antibiotic doxycycline.[47] Unlike anthrax, plague is highly communicable; an infected individual may spread infection by coughing. Its capability to lead to an epidemic may be an advantage to someone seeking to generate mass havoc, but it may be a disadvantage to someone planning a more strategic strike. In contrast to anthrax, plague bacteria have the disadvantage of being subject to environmental stress, complicating dissemination.

d. Haemorrhagic Fevers

Rift Valley Fever (RVF) is a viral disease prevalent among livestock. The virus is spread by mosquitoes to animals. Infected animals then become new hosts for other mosquitoes that in turn become additional vectors for transmission. These mosquitoes can then infect humans. RVF victims tend to experience symptoms associated with a mild illness such as fever, dizziness, and back pain. In some people, the illness can progress into hemorrhagic fever, encephalitis, or ocular disease, but most patients recover from exposure within a few days. A terrorist's mishandling may lead to unintentional exposure, with no known treatment.

Marburg Hemorrhagic Fever affects humans and other primates in very localized areas. Like the plague, the virus is highly infectious. Humans can contract the disease from handling monkeys, from droplets of body fluids, or contact with contaminated people or other sources of infectious blood or tissues. Symptoms appear five to ten days after exposure. Death ensues rapidly. This virus may appeal to the potential terrorist for its 25% mortality rate, but knowledge of the virus and proper handling are necessary to prevent risk to oneself.

The ebola virus is known for its horrific symptoms: vomiting, chest pain, and bleeding from virtually every orifice.[48] The disease is spread through close personal contact with an

47. *See id.*

48. *See* Sean Henahan, *Dr. Frederick A. Murphy Talks About the Ebola Virus*, Access Excellence, *at* http://www.accessexcellence.org/WN/NM/interview_murphy.html (last visited January 5, 2001) (interview with Dr. Frederick A. Murphy, Dean of School of Veterinary Medicine, UC Davis).

infected victim. Transmission has also been known to take place through hypodermic needles. The ebola virus is similar to the Marburg virus but has a lower infection rate. Humans are susceptible to several different strains; the more lethal strains are the less contagious.

e. Tularemia

Tularemia (*Francisella tularensis*) is an extremely lethal bacterium spread by insect bites from rodents to humans. A virulent form (fatality rate of approximately 5%) is endemic in much of North America and can be obtained from dead animals; a pneumonic form, which would result from an intentional release, would likely have a greater mortality rate.[49] Propagation would require special media as tularemia does not typically grow in standard blood cultures. It is not transmitted person-to-person, eliminating the possibility of epidemic. Treatment is typically effective by common antibiotics within seven to fourteen days of infection, making treatment and containment by public health authorities possible. Moreover, like plague, it is subject to environmental stresses.

f. Venezuelan Equine Encephalitis

Venezuelan Equine Encephalitis (VEE) is a mosquito-borne virus. A large controlled mosquito population could feed on an infected animal and become the vector to transfer the virus to humans. Susceptibility to this disease is nearly 100%; however, its mortality rate is less than 1%, making it an unlikely choice for a weapon. An infected human remains infectious for mosquitoes for at least seventy-two hours after symptoms, enabling secondary spread of the disease. Infected individuals who do not seek treatment may progress into encephalitis, which is marked by convulsion, coma and paralysis. A human vaccine is available through USAMRIID.[50]

g. Ricin

Ricin is an inanimate protein toxin that may be readily produced from castor beans. It acts as a cellular poison that is lethal either through inhalation or through epidermal

49. *See* U.S. Army Inst. of Infectious Diseases, *supra* note 30.
50. *See id.*

absorption. A tiny quantity on the skin rapidly causes death. Ricin may be used to poison water or foodstuffs or lace injectiles. Ricin has a long record of use by assassins because the victim need only be poked by an object coated with the toxin.[51] If ricin is inhaled, fever, coughing, and nausea occur within eight hours and death ensues within thirty-six to seventy-two hours. Notably, there is no treatment; once a victim is poisoned, death will follow. There is no vaccine, so a terrorist would have to be extremely sophisticated to avoid suicide. Since it is non-contagious, it has no ability to provoke an epidemic, yet it may be the most easily disseminated pathogenic agent and therefore one of the most effective means of committing murder.

2. *Choosing the Appropriate Pathogen*

No single agent is ideal for terrorism. A terrorist must make choices depending on what he is trying to accomplish as well as his level of technical knowledge and equipment.

If the goal is to murder an individual or small group of people, ricin may be uniquely suitable. Ricin is easily produced from widely available castor beans. Because it kills by epidermal contact, it is likely that the murderer will remain anonymous. However, there is no shortage of guns, knives, conventional poisons etc. available to the terrorist who wishes only to kill a small number of people; producing ricin may not be worth the time and risk.[52]

If the terrorist's goal is mass murder, anthrax deserves its reputation as perhaps the most feared biological weapon. It is readily available. Disseminated in a closed, positive air pressure environment, anthrax could get into the lungs of most people in that environment. By the time symptoms become obvious, it would be difficult, even with a full commitment of health care resources, to prevent a high number of deaths. In other settings, however, the difficulties of suspending anthrax outdoors and the unlikelihood of it spreading from one victim to another render it a poor open-air, urban-devastating weapon.

---

51. *See* FALKENRATH ET AL., *supra* note 2, at 81 n.125 (citing numerous articles discussing assassinations and attempted assassinations using bio weapons).

52. *See id.* at 16.

If the terrorist's goal is contagion, plague is almost as readily available as anthrax and is contagious, although it is less resilient to environmental stresses and more difficult to cultivate.[53] More esoteric are viruses including encephalitis or any of the extremely deadly hemorrhagic fevers. These viruses are far more difficult to obtain, and the knowledge of how to propagate them safely is far more limited. Moreover, as these viruses are not available domestically, the terrorist would have to go to some other part of the globe and bring at least some agent through customs, thereby risking detection.[54] The organisms of brucellosis are difficult to grow, but are highly infectious and relatively stable for aerosolization. The tularemia organism is also extremely infectious; however, it is difficult to grow and is delicate when disseminated.[55]

If the terrorist's goal is a weapon of mass destruction, smallpox has attributes of contagion and lethality that are unmatched by any other natural agent. However, smallpox is available, if at all, only from unsecured Russian laboratories. To obtain and transport it into the United States would entail an organized conspiracy more akin to an act of war than an act of terrorism. Sophisticated bio-engineered agents, whether animate or toxin, are similarly effective but require foreign assistance in order to be obtained. The good news here is that using biological agents as a weapon of mass destruction seems to be well beyond the capabilities of domestic hate groups or the likes of a Tim McVeigh or Ted Kaczynski ("The Unabomber").

C. Devising the Attack

How difficult it is to make biological weapons and how much sophistication is required are matters in sharp dispute. According to some experts, medical or microbiology students could prepare an agent without endangering themselves.[56] But making that agent into a weapon by aerosolizing it requires considerably greater sophistication. Many experts believe that

53. *See* Purver, *supra* note 2.

54. *See id.*

55. *See id.*

56. U.S. OFFICE TECH. ASSESSMENT, TECHNOLOGY AGAINST TERRORISM: STRUCTURING SECURITY 37 (1992), *available at* http://www.wws.princeton.edu/~ota/ns20/year_f.html.

the difficulties of executing a mass biological attack explain why such a successful catastrophic attack has not yet occurred.[57] Persons having extraordinary technical knowledge may be able to overcome problems of deficient resources and equipment, but there is a negative correlation between capability to use pathogens and a motivation to cause mass casualties.[58]

1. Means of Acquisition

A seed culture could be obtained from a legitimate facility either by purchasing it or stealing it, from the natural environment, or by importing it. Purchase of pathogens was once not difficult, but controls have recently been significantly tightened, as will be discussed at length below. As discussed below, the stealing of agents raises serious problems, including alerting law enforcement authorities to the risk of an attack. Therefore, access to these agents may require the services of someone affiliated with the laboratory or facility.

The most likely means of acquiring pathogens are from a natural or a foreign source. Either of these means, as distinct from buying or stealing pathogens, is virtually unstoppable. Within the United States, agents such as anthrax and plague and tularemia as well as variety of toxins, can be obtained from dead animals or vegetable matter.[59] Resort to this method minimizes the risks of detection as well as the financial cost. However, identifying a strain that can be effectively weaponized and then proceeding to weaponize it requires considerable sophistication as well as equipment. Procurement from a foreign source is a virtually foolproof solution to the task of acquisition, although smuggling the material into the United States poses risks of detection. Unless the agent is already weaponized (which would increase the danger and detectability of smuggling it), it would have to be weaponized here. In that respect, obtaining an agent from a foreign source

57. *See, e.g., Assessing the Threat of Bio-terrorism: Hearing Before the House Government Reform Committee,* 106th Cong. (1999) (statement of Raymond A. Zilinskas); Jonathan B. Tucker, *The Chemical and Biological Threat,* CURRENT HISTORY, April 2000, at 147.

58. *See* STERN, *supra* note 4, at 77.

59. *See* Emil Lesho et al., *Feces, Dead Horses, and Fleas: Evolution of the Hostile Use of Biological Agents,* WESTERN J. MED., June 1998, at 512.

poses problems similar to obtaining it from a natural source, although the agent is likely to be of a higher quality.

2. *Means of Production*

Once the agent has been obtained, it must be cultured. The difficulty in producing enough of the agent to create a weapon may present an important limitation to terrorism, because some methods may be too advanced for terrorists.[60] Moreover, agents are fragile; production would require favorable conditions. For instance, the terrorist would need the appropriate media, the right temperature, pressure and atmospheric conditions, and the ability to maintain this environment for the necessary time for the particular agent. For bacteria, growth and production imply taking a small isolate (perhaps a test tube) and growing a large quantity that can be used in a weapon. The actual quantity of material required to produce an effective weapon depends on many factors, not least of which is the strain's virulence. Although some organisms are known to cause disease when infected with fewer than 100 cells (*Pseudomonas*), higher concentrations increase the chance of infection. Therefore, large volumes of highly concentrated material are required for a biological weapon.

The scientific proficiency required to culture an agent is a factor in agent selection. Growth and media requirements and techniques for production for pathogenic microorganisms are easily researched. The pathogenesis of these organisms has led to intensive study of growth characteristics and requirements, which are now well understood and published. However, obtaining the growth media used in traditional research, as well as the clinical setting, presents a significant hurdle in creating a biological weapon. For instance, *Yersinia pestis*, the bacterium that causes plague, is difficult to grow on any media other than blood agar.

3. *Means of Dissemination*

The means of delivery will depend on the number of people

60. *See* Robert Taylor, Bio-terrorism Special Report—All Fall Down, *at* http://www.sightings.com/political/weapons/allfall.htm (May 12, 1998) (describing accessibility of production, including brewing several kilograms of slurry containing billions of spores).

the terrorist seeks to reach and his ability to successfully weaponize the agent. For instance, dissemination by aerosolization, as opposed to delivering a sealed box of dry powder agent leading to infection if inhaled, requires knowledge and skill with regard to how to minimize the particle size of the agent and spread it in a fine cloud. Yet the requisite technology, laboratory facilities, and aerosolization devices are within the grasp of even the weakest countries.[61]

Commentators differ as to the difficulty of disseminating biological agents.[62] Biological agents can be disseminated individually through inanimate objects such as sticks, dusters, or projectiles. But if one seeks to spread disease to many people, the more common methods of dissemination of biological agents include aerosol delivery, dry-powder delivery, spraying, infecting food and water supplies, and introducing insect or animal vectors. The bioterrorist must choose an agent that has infectious capabilities but does not kill its host quickly. The fragile nature of the agents themselves can impede any dissemination effort;[63] preparing and preserving the agent before dissemination can affect its ability to survive spraying and cause disease. Mechanical stresses and exposures to air, humidity, and ultraviolet light rapidly kill many microorganisms.

These considerations, in turn, will also contribute to the chosen route of dissemination. For instance, living

---

61. *See* Purver, *supra* note 2.

62. *Compare* Cole, *supra* note 2, at 61 (concluding that a major biological arsenal could be built with $10,000 worth of equipment in a room 15 feet by 15 feet), *and* U.S. OFFICE TECH. ASSESSMENT, TECHNOLOGIES UNDERLYING WEAPONS OF MASS DESTRUCTION 71-117 (1993) ("[A] sophisticated delivery system may not be required. Biological agents can be disseminated by cross-winds with few, if any, indications of hostile intent. Commercially available equipment, such as agricultural sprayers, can be used to attack broad area targets."), *available at* http://www.wws.princeton.edu/~ota/ns20/alpha_f.html, *with Worldwide Biological Warfare Threat*, *supra* note 29 ("[T]he preparation and effective use of [biological weapons] . . . is harder than some popular literature seems to suggest.").

63. Outdoor aerosol delivery is sensitive to weather, air, humidity, and ultraviolent rays. "[A]gents are inherently susceptible to environmental insults including desiccation, humidity, and oxidation." Janice Sung, *Understanding the BW Threat*, Carnegie Endowment for Int'l Peace, *at* http://www.ceip.org/programs/nnp/brief211.htm (July 1, 1999); *see also* Pearson, *supra* note 18 ("If bombs or rockets are employed to disseminate the agent, explosives will probably be used to open the munition and to disperse the agent into the atmosphere. The detonation of the explosive produces heat and shock, which can kill the living microorganisms.").

microorganisms may enter the human body by an aerosol route, where they invade the respiratory tract, enter the bloodstream and lymphatic system, and then initiate infection; anthrax is not really infectious except by the aerosol route. By contrast, toxins affect people through direct exposure; they have no infectious characteristics but rather must be ingested, injected or inhaled.[64]

a. Injection or Direct Poisoning

Almost all of the known incidents of hostile use of pathogens or toxins have involved direct injection or poisoning of an individual. This method of dispersion, referred to as "point source,"[65] occurs where the enemy spews a biological agent directly on the target. Ricin-tipped umbrellas have been used for clandestine espionage and counter-intelligence, and popular novels have illuminated the implications of murder-by-biology. These incidents are cited as evidence of how easy it is to make lethal biological agents, but there are prodigious technical differences between homicide and mass catastrophe. As earlier stated, guns are remarkably easier and cheaper to obtain and use.

b. Contamination of Foodstuffs or Potable Liquids

The easiest way to distribute pathogens is to spread them on foodstuffs. Most examples of successful biological terrorism have involved spreading food-borne diseases (e.g., salmonella) on openly accessible food sources such as salad bars.[66] This type of attack is virtually impossible to prevent once the terrorist has developed the agent and has obtained access to the food source. Yet this type of attack is not likely to cause a catastrophic number of injuries; indeed, experience with this type of attack suggests that casualties are more likely to

64. *See* U.S. OFFICE TECH. ASSESSMENT, *supra* note 29, at 35.

65. Linda D. Zozaryn, *Defending Against Invisible Killers—Biological Agents*, DefenseLINK, *at* http://www.defenselink.mil/specials/chembio (last modified January 11, 2001).

66. *See, e.g.*, Cole, *supra* note 2, at 61-62 (noting that in 1984 a cult poisoned Oregon salad bars with salmonella, making 750 people sick); *see also* Laura Beil, *Biological Attack Poses a Real Threat, Experts Say; Risk Is Believed To Be Small, But Civilians Could Be Target*, DALLAS MORNING NEWS, May 23, 1999, at 1A (noting that in 1996 a lab worker at St. Paul Medical Center dumped *shigella bacteria* on a co-worker's pastries).

number in the dozens than the thousands. The most infamous known event of this type was in 1984 when the Rajneesh cult outside of Antelope, Oregon, poisoned 750 people with salmonella at local salad bars. Attacks through bulk foodstuffs or beverages have been discussed, but most experts believe that such a mass attack is unlikely.[67]

Contamination of water supplies is considerably more difficult in countries which have efficient water purification systems (such as the United States) because of the extraordinary quantities of pathogens necessary and because filtration and chlorinated purification systems would likely kill the agent.[68] Notably, Chicago-area neo-nazis were arrested in 1972 with thirty to forty kilograms of typhoid bacteria for use against water supplies. That a few college students could cultivate this disease in a school laboratory provoked considerable concern, but their selected organism would have been readily destroyed by normal chlorination. This distribution method, however, could be effective in less-developed regions.

c. Aerosol Delivery

A terrorist employing biological weapons for a large-scale attack with many casualties will most likely distribute pathogens as an aerosol through airborne transmission.[69] Experts differ as to how difficult aerosolization is likely to be. While most experts recognize the ready availability of aerosolization equipment (discussed below), there is considerable difference of opinion as to the level of expertise needed to produce an aerosol generator capable of weaponizing pathogens.[70]

---

67. *See* Laurie Garrett, *Weapons in the Hands of a Cult/Group Plotted Attack To Influence Election*, NEWSDAY, Apr. 6, 1998, at A24.

68. *See Terrorist & Intelligence Operations: Potential Impact on the U.S. Economy: Hearing Before the J. Economic Comm.*, 105th Cong. (1998) (statement of Dr. Kenneth Alibeck, Program manager, Battelle Memorial Institute), *available at* http://www.house.gov/jec/hearings/intell/alibek.htm.

69. Airborne transmission is when infectious agents are spread as aerosols and enter a person, usually through the respiratory tract. Aerosols are tiny particles, consisting in part of the infectious agent itself, which becomes suspended in the air. *See* Centers for Disease Control & Prevention, Glossary of Terms, *at* http://www.cdc.gov/ncidod/dvrd/spb/mnpages/glossary.htm (last visited January 5, 2001).

70. *Compare* Purver, *supra* note 2:

Outside aerosol delivery highlights contrasting opinions. An effective delivery system must have two major attributes. First, the delivery system needs to expel the agent efficiently from its container so that it will travel to potential targets. Second, assuming the agent attacks through the respiratory system, the delivery system must produce small particles that will be retained on inhalation. Ranges of one to ten microns are required because larger particles settle out of the atmosphere rapidly and are not inhaled.[71] Paint spray devices are ineffective because of their large particle size. Also because of the necessity of small particle size, a terrorist employing agricultural spraying as his method of dissemination will have to address the problem of decreasing the particle size. Agricultural sprayers expel droplets of a size range that will fall onto the crops. By contrast, smaller particle sizes are necessary to produce an aerosol cloud which will suspend above the surface level.

Even if the terrorist can accomplish this successfully, a hardy agent is still required to survive the expulsion from a sprayer long enough to infect the intended targets. Outdoor aerosol delivery of biological weapons is acutely sensitive to weather conditions, the quality of the dispersal system, and the characteristics of the agent used, making aerosol dissemination of all but a few hardy species technologically challenging.[72] The stress of the aerosolization process itself can kill a large portion of the pathogen; atmospheric conditions such as moisture, sunlight, smog, and temperature changes can take an enormous toll. A nighttime dissemination under stable meteorological conditions would improve chances of success. A cloud released to drift over a densely populated urban area

---

> Aerosol dispersal technology is easy to obtain from open literature and commercial sources, and equipment to aerosolize biological agents is available as virtually off the shelf systems produced for legitimate industrial, medical, and agricultural applications. With access to a standard machine shop, it would not be difficult to fabricate aerosol generators and integrate components to produce reliable systems for dispersing microorganisms or toxins.

with Beil, *supra* note 66 (quoting Dr. Philip Brachman, medical epidemiologist, "'You'd have to really know what you were doing to be able to develop an aerosol. It would take an unusual bit of equipment'").

71. *See generally* Centers for Disease Control and Prevention, *Bio-terrorism*, 5 EMERGING INFECTIOUS DISEASES (1995), *available at* http://www.cdc.gov/ncidod/eid/vol5no4/contents.htm.

72. *See* FALKENRATH ET AL., *supra* note 2, at 123.

during a mild winter night would probably be most effective; a light wind to prevent the aerosol from settling and an inversion layer to confine the cloud to lower altitudes would aid dissemination.

Somewhat more effective is aerosol dissemination in an indoor setting such as by gaining access to the air circulation system of an office building or public arena. The U.S. Army demonstrated the effectiveness of this delivery system by releasing harmless bacteria into New York City subways.[73]

d. Animal and Insect Vectors

Vectors are normally insects that carry a host of different infectious agents, but a vector can be any creature that transmits an infectious agent to humans when it bites or touches a person.[74] The infectious agent may be injected with the insect's salivary fluid when it bites, or an insect may regurgitate material or deposit feces on the skin that enter a person's body, typically through a bite wound or skin broken by scratching or rubbing. Once the agent is within the vector animal, an incubation period follows during which the agent grows or reproduces, or both, depending on the type of agent. Only after this phase is over does the vector become infectious.

A highly contagious pathogen could be propagated in a dead animal, and then large numbers of insects could be exposed to that carcass in a confined space, collected, and then released in a population center. Allegedly, the Soviet Union had

---

73. *See* Elliott J. Schuchardt, *Walking a Thin Line: Distinguishing Between Research and Medical Practice During Operation Desert Storm*, 26 COLUM. J. L. & SOC. PROBS. 77, 99 (1992) ("[I]n 1966, the Corps sprayed innocuous bacteria into New York City's subway to determine how far bacteria could be transmitted in this manner. Within minutes, the turbulence caused by the passing trains carried the germs throughout the entire rail system."). Schuchardt notes:

> Not all of the tests were harmless, however. In September 1950, the Army Chemical Corps conducted a mock germ warfare attack on San Francisco. Over six days, the Corps contaminated 117 square miles with *Serratia marcescens*, a strain of bacteria then believed to be harmless to humans. Over the next five months, a San Francisco hospital treated eleven cases of infection caused by this normally benign bacteria. While the Army claims this outbreak was purely "coincidental," it is now known that *Serratia marcescens* poses a serious hazard to individuals with certain predisposing factors.

Id. (citations omitted).

74. *See* Centers for Disease Control & Prevention, All About Hantavirus, *at* http://www.cdc.gov/ncidod/diseases/hanta/hps/index.htm (June 1, 1999).

researched this dissemination method,[75] but there is scant evidence that terrorists have mastered it. More recently, Cuba accused the United States of committing a biological attack by distributing disease-carrying insects from aircraft.[76]

Using insect vectors overcomes the difficulties of aerosolizing pathogens, but the use of insects is necessarily unreliable. Significantly, because only a few pathogens (notably the tropical viruses) are transmittable through this method, a terrorist would reduce options by using insects. To be effective, a highly contagious pathogen must be selected, raising the risk of self-contagion.

4. Assessing the Risk

It would verge on pure speculation to assert that the risk of a particular biological attack is significant or not. Conversations with U.S. government officials suggest that staging a biological attack is far easier than using a nuclear device, even a crude one. But there is no way to confirm or measure this risk. Decisions on appropriate policies must be made, therefore, in a condition of some uncertainty. Yet it should be noted that the direction of biological understanding renders current estimates somewhat irrelevant as to future capabilities. Even sophisticated biologists in the 1980s would have been hard pressed to predict the quality and magnitude of today's bio-engineering; implementation of policies to address threats are likely to follow a somewhat slower progress.

II. RESTRICTING ACCESS TO PATHOGENS AND WEAPONIZING EQUIPMENT

Because few pathogens are useable for catastrophic terrorism and because making biological weapons is a complex undertaking, it makes sense to implement regulations to deny potential terrorists access to critical agents and equipment. But these items are dual use—they have legitimate research and commercial applications. Thus, efforts to prevent bioterrorism would likely intrude on the activities of the bio-pharmaceutical

75. *See* KENNETH ALIBEK, BIOHAZARD: THE CHILLING TRUE STORY OF THE LARGEST COVERT BIOLOGICAL WEAPONS PROGRAM IN THE WORLD, TOLD FROM THE INSIDE BY THE MAN WHO RAN IT (1999).

76. *See* Susan Wright, *Cuba Case Tests Treaty*, BULL. ATOM. SCIENTISTS, Nov.-Dec. 1997, at 18.

sector, and serious thought should be given to the appropriate degree of that intrusion. More precisely, since the bio-pharmaceutical sector has capabilities to make biological weapons, and since diversion of those capabilities to such purposes could have horrifying consequences, what constraints should be placed on that sector?

Answering this question entails assessments of the risk of a bioterrorist attack, the likelihood that the bio-pharmaceutical sector might contribute to that attack (wittingly or not), the need for active cooperation by the bio-pharmaceutical sector in counter-terrorism efforts, the likely efficacy of regulatory measures, and the ancillary costs of those measures as well as their drag on socially useful activity. Reasonable minds may reach different estimations.

One viewpoint argues, with considerable merit, that the horror of mass disease justifies taking actions that might reduce the risk. An alternative viewpoint warns, also with considerable merit, that burdening research and industrial activity is unwarranted because of the low probability of an actual attack.[77] Unfortunately, these viewpoints tend to talk past each other, complicating progressive policies. There is an undeniable need for highly-nuanced analyses of this problem.

The anchoring position of this Part should not be controversial: The bio-pharmaceutical sector is a crucial ally in efforts to prevent bioterrorism. This sector must perform basic research on pathogenicity and virology, produce vaccines and antidotes and instruct first responders on their use, and join with other disciplines to create sensing capabilities[78] to assist law enforcement. Moreover, the bio-pharmaceutical sector is among the most regulated, but that regulatory system is directed almost exclusively at protecting the public against dangerous products, not at denying terrorists the wherewithal

77. *See* Ehud Sprinzak, *The Great Superterrorism Scare*, FOREIGN POL'Y, Fall 1998, at 110, 118-19; *see also* Chitra Ragavan & David E. Kaplan, *The Boom in Bioterror Funds*, U.S. NEWS & WORLD REP., Oct. 18, 1999, at 24-25. *See generally* Arnold F. Kaufmann, Martin I. Meltzer & George P. Schmid, *The Economic Impact of a Bioterrorist Attack: Are Prevention and Postattack Intervention Programs Justifiable?* 3 EMERGING INFECTIOUS DISEASES 83 (1997) (discussing the economic impact of biological agents and the efficacy of responses to them).

78. *See* Joseph Alper, *From the Bioweapons Trenches, New Tools for Battling Microbes*, SCIENCE, June 11, 1999, at 1754 (describing the need for a device to "sniff out" and "identify pathogens quickly enough to save lives during a bioterrorist attack").

to fulfill their evil plans.

Many notable experts believe that terrorists can order pathogenic seed cultures from laboratories or through the mail. "[C]ommercial firms offer cultures for a few dollars, and they rarely check whether those placing an order are acquiring it for a legitimate use."[79] Recently, however, this has changed; transmittal of pathogens is now strictly controlled. Similarly, theft or diversion of pathogens from laboratories or in transit is not currently an easy proposition, although measures could be implemented to fortify current safeguards. More problematic is the lack of a system to prevent bioterrorists from gaining access to useful equipment.

The following discussion addresses measures to deny access to pathogens and to critical weaponization equipment. A single guiding principle runs throughout the discussion: To the extent regulatory modifications can reasonably diminish the possibility of a group obtaining and weaponizing pathogens, the commercial/research sector should embrace those modifications as the price of living in a dangerous world; to the extent terrorists can develop bioweaponry without turning to the commercial/research sector, regulatory burdens might not diminish risks—it makes more sense to cooperate with industry than to weigh it down in the name of "doing something."

A. Restriction of Access to Pathogens

Most biological pathogens are legitimately supplied by a few commercial companies such as the American Type Culture Collection (ATCC), a private organization that distributes the agents for biological use to pharmaceutical companies, universities, and medical laboratories.

Before 1996, the regulatory system controlling access to and dissemination of biological agents was designed, virtually exclusively, to prevent public distribution of unsafe pharmaceutical or other biological products. It was not expressly designed to prevent terrorist use of biological agents. Consequently, wrongful access to such agents was easier than it should have been.[80]

---

79. LAQUEUR, *supra* note 3, at 67.

80. *See* Purver, *supra* note 2 ("Until recently, all desired strains of viruses or

1. Larry Wayne Harris

The modern era of regulatory law to prevent access to biological weapons begins with Larry Wayne Harris. In 1995, Harris, a microbiologist, a lieutenant in the neo-nazi organization Aryan Nations, and a governing board member of the National Alliance, ordered *Yersinia pestis* (the cause of bubonic plague) from ATCC. Harris lacked a license, but he identified himself as under contract with the State of California. He opened an account using stationery he had prepared with the letterhead of a non-existent laboratory. He indicated that he was trained to handle Class 3 cultures, and requested *Yersina pestis* for research on rats to develop an over-the-counter antidote for bubonic plague. Freeze-dried plague was shipped to his home.

One day after shipment, an ATCC technician, concerned that Harris might not handle the requested material safely, notified the Centers for Disease Control (CDC), which phoned Harris. Harris explained that his research was designed to counteract "Iraqi rats carrying 'supergerms.'"[81] He further revealed that he was writing a survivalist manual in his home laboratory in a residential neighborhood. One week later, the CDC along with local police obtained a search warrant and found three vials of pathogens in his car as well as weapons and explosives in his home. When confronted, Harris professed that Armageddon is imminent and that stockpiled weapons are necessary to survive.[82] Subsequently convicted of wire fraud for having misrepresented his status to the lab when ordering the plague, Harris was sentenced to eighteen months probation.[83]

---

bacteria could be purchased without any problem from the American Type Culture Collection (ATCC).") (quoting Karl-Heinz Karisch, *The Fear of the Return of German Exports*, *in* FRANKFURTER RUNDSCHAU 6 (1991)). Purver writes:

> Some organisms—including most of those suitable for biological warfare—are restricted, but this means only that the person ordering must be confirmed as a qualified investigator. The controls are not tight: the signature of a laboratory or department head is sufficient proof. It would be about as difficult as forging a prescription for an unqualified person to obtain these cultures.

Id. (quoting BRIAN M. JENKINS & ALFRED P. RUBIN, NEW VULNERABILITIES & THE ACQUISITION OF NEW WEAPONS BY NONGOVERNMENTAL GROUPS 226 (1978)).

81. Cole, *supra* note 2, at 61.

82. *See* Jessica E. Stern, *Larry Wayne Harris: The Talkative Terrorist*, *in* TOXIC TERROR: ASSESSING THE TERRORIST USE OF CHEMICAL & BIOLOGICAL WEAPONS 139 (Jonathan Tucker ed., 2000).

83. United States v. Harris, 961 F. Supp. 1127 (S.D. Ohio 1997).

The Harris incident warned policy makers that it was too easy to obtain pathogenic seed cultures. After Harris acquired his pathogenic agents, the CDC tightened existing regulations pertaining to the acquisition, transfer, packaging, labeling, or handling of biological agents to reduce the possibility that biological pathogens could be fraudulently ordered from these commercial suppliers.[84]

2. *Licensing Possession of Pathogenic Agents*

A complicated regulatory system confines legitimate possession of pathogens to highly controlled facilities in order to prevent releases of dangerous products into the marketplace. Any biological products entering the marketplace must be licensed, and the facilities where they are manufactured must be licensed as well. Persons requesting licenses must be closely screened because of their access to these pathogens.

a. *Establishment Licenses*

Manufacturers must have a valid license that allows them to work with pathogenic agents so long as their establishment complies with regulations on manufacturing and testing.[85] A laboratory must apply for registration to work with the agent and abide by the recommendations laid out in the Centers for Disease Control publication, *Biosafety in Microbiological and Biomedical Laboratories* (*Biosafety Manual*), which categorizes infectious agents and laboratory activities into four classes or levels.[86] Each establishment attempting to obtain or work with

---

84. *See infra* notes 88-89; *see also Bio-terrorism: Hearing Before the Senate Appropriations Comm., Subcomm. on Labor, Health and Human Servs., Education, and Related Agencies*, 106th Cong. (1999) (testimony of Margaret A. Hamburg, M.D., Assistant Secretary for Planning and Evaluation, Department of Health and Human Services) [hereinafter *Bio-terrorism: Hearing Before the Senate Appropriations Comm.*]; *Hearing Before the Senate Comm. on Intelligence, the Subcomm. on Technology, Terrorism, and Gov't Information Comm. on the Judiciary*, 105th Cong. (1998) (statement of Stephen M. Ostroff, M.D., Director of Epidemiologic Science, Centers for Disease Control and Prevention).

85. *See* 42 U.S.C. § 262(a) (2000). An establishment license is required for all those working with biological agents except for laboratories used for research, diagnostic, reference and/or verification purposes. These laboratories must be certified but do not require a license. *See infra* notes 90-97, and accompanying text.

86. *See* NAT'L CENTER INJURY PREVENTION & CONTROL, OFFICE OF HEALTH & SAFETY, BIOSAFETY IN MICROBIOLOGICAL AND BIOMEDICAL LABORATORIES (Jonathon Y. Richmond et al. eds., 4th ed. 1999), *available at* http://www.cdc.gov/od/ohs/irsat/42cfr72.html [hereinafter BMBL]. The Manual has detailed instructions to guide laboratory directors to develop better methods of handling

select agents must certify that its facility meets these requirements.[87] Licensees must keep detailed records that give a complete accounting of activities within each establishment.[88]

The requirements of a biosafety level 1 laboratory apply to agents that do not ordinarily cause human disease. By contrast, level 3 requirements apply to agents that can cause serious infection that may be transmitted by the respiratory route. The most dangerous and therefore the most protected environments are level 4 laboratories, used for the diagnosis of exotic agents that pose a high risk of life-threatening disease, that may be transmitted by the aerosol route and for which there is no vaccine or therapy.[89] Recommendations are set out according to the laboratory level defined by the agents it handles and to specific guidelines for each agent. These requirements dictate methods for protection of agents and security from outsiders, i.e., potential terrorists.

b. Product Licenses

A license is required for each biological product to be released into commerce.[90] The product must be safe, pure, and

---

storing, containing, and sterilizing infectious agents. *See Bio-terrorism: Hearing Before the Senate Appropriations Comm.*, *supra* note 84.

87. Compliance with the Biosafety Manual is not overtly obligatory, but under OSHA regulations, agents must be secured and handled consistent with the Manual's instructions to ensure a safe laboratory. Where a facility fails to follow the guidelines and an accident or release of an agent occurs, the owner will be held liable. Significantly, each laboratory director is personally responsible for the safety of laboratory employees. Therefore, while not obligatory, any actions inconsistent with the Manual resulting in harm, may render the director liable. *See id.*

88. *See* 9 C.F.R. § 116 (2000). The establishment must keep records concurrently with each step of the manufacturing process and submit information about the quantity and identity of the product, and the circumstances and actions taken for any indications raising questions about the purity, safety, potency, or efficacy of the product. *See id.*

89. Requirements differ according to certain biosafety levels, in order to make it more difficult to be in contact with highly lethal, infectious agents. Biosafety levels are specific combinations of work practices, safety equipment, and facilities, which are designed to minimize the exposure of workers and the environment to infectious agents. The guidelines can be customized for each individual laboratory and can be used in conjunction with other available scientific information on risk assessment to further minimize the potential for laboratory associated infections. The latest edition of the BMBL specifically describes combinations of microbiological practices, laboratory facilities, and safety equipment, and recommends their use in four categories or biosafety levels of laboratory operation with selected agents infectious to humans. *See* BMBL, *supra* note 86, tbl. 1 (Summary of Recommended Biosafety Levels for Infectious Agents).

90. *See* 21 C.F.R. §§ 601.12(a), 601.20 (2000).

potent; the facility from which it is manufactured must meet standards designed to ensure those attributes.[91] License holders of biologics must maintain concurrent records with each step in manufacture and distribution and submit information about the quantity of each licensed product every six months.[92] Lastly, the applicant must consent to inspection of the product and the facility by the department's inspectors.[93] The department must maintain product samples and summaries of all the clinical and non-clinical studies.[94]

c. Registration Controls of Transferring Agents

Obtaining pathogenic agents is no longer an easily manipulated process. Suppliers of select agents that seek to transfer or receive agents are required to register with the CDC and obtain a registration number. Both the transferring and requesting entities must be registered as equipped and capable of handling the agents.[95] Facilities attempting to purchase biological agents, except clinical laboratories,[96] must give their license number in order to obtain biological agents.[97] All CDC

---

91. *See* 21 C.F.R. § 601.20 (2000). The product must undergo testing in order to be declared safe, pure and potent; test results are reviewed by the department before the product may be distributed. *See* 21 C.F.R. § 601.3 (2000).

92. *See* 21 C.F.R. § 600.81 (2000).

93. *See* 42 U.S.C. § 262(c) (2000); *see also* 21 C.F.R. §§ 600.20-22 (2000) (detailing establishment inspections requirements).

94. *See* 21 C.F.R. § 600.13 (2000).

95. *See* 42 C.F.R. § 72.6(a)(1) (1999). The rule for transfers is in accordance with the licensing requirements under 42 U.S.C. § 262 (2000). This provision was the result of the Antiterrorism and Effective Death Penalty Act of 1996, which imposed upon the Center for Disease Control an obligation to take action. *See Bioterrorism: Hearing Before the Senate Appropriations Comm., supra* note 84. The Act established new provisions to regulate transfer of hazardous agents, and required the Secretary of Health and Human Services to promulgate implementing regulations. The regulation amended existing requirements for packaging, labeling and transport of select agents, and placed additional shipping and handling requirements on facilities that transfer or receive 'select agents' that are capable of causing substantial harm to human health. *See Biological Weapons: Hearing of the Senate Select Intelligence Committee*, 105th Cong. (1998) (statement of Stephen M. Ostroff, M.D., Associate Director for Epidemiologic Science, National Center for Infectious Diseases).

96. *See* 42 C.F.R. § 72.6(h)(2) (1999) (exempting certified clinical laboratories that use an agent for diagnostic, reference, verification, or proficiency testing purposes).

97. *See* 42 C.F.R. § 72.6(d)(1)(iv) (1999). The facility must be certified as meeting the biosafety level standard as dictated by *Biosafety in Microbiological and Biomedical Laboratories*. *See* 42 C.F.R. §§ 72.6(a)(1), 72.6(a)(5) (1999). Prior to the transfer of any agent a CDC Form EA-101 must be completed. These forms require the name of the requestor and receiving facility, the name of the transferor

forms EA-101 must be produced upon request to appropriate federal and authorized local law enforcement authorities, officials authorized by the Secretary, and officials of the registering entity. Prior to transferring any agent, the transferor's responsible facility official must verify with the requestor's responsible facility official (and, as appropriate, with the registering entity) that the requesting facility retains a valid, current registration, that the requestor is an employee of the requesting facility, and that the proposed use of the agent by the requestor is correctly indicated on CDC Form EA-101. Upon completion of the CDC Form EA-101 and verification of registration, the transferring facility must comply with the packaging and shipping requirements when transferring the agent. The requesting facility's responsible official must acknowledge receipt of the agent within thirty-six hours of receipt and provide a paper copy or facsimile transmission of receipt to the transferor within three business days of receipt of the agent.

3. *Preventing Theft of Pathogens*

Although deadly agents can no longer be ordered from legitimate sources, the possibility of theft remains. An outsider can break into a secure site or steal material while it is in transit. Alternatively, an insider (a 'mad scientist') can divert agents to impermissible uses. Therefore, additional security for biological agents is important to prevent and deter potential terrorists from surreptitious acquisition of pathogens.

a. Facility Regulations

Facilities housing biological agents may be inviting targets of theft for bioterrorists. The purpose of containment—safe methods to manage infectious agents in the laboratory where they are handled or maintained—is to reduce or eliminate the

---

and transferring facility, the names of the officials responsible for both the transferor and requestor, the requesting and transferring facilities' registration numbers, the agent being shipped, the proposed use of the agent, and the quantity of agent shipped. *See* 42 C.F.R. § 72.6(d)(1) (1999). The form must be signed by the transferor, requestor, and the responsible facility officials representing both the transferring and requesting facilities. *See* 42 C.F.R. § 72.6(d)(2) (1999). A copy of the completed CDC Form EA-101 must be retained by both transferring and requesting facilities for five years after the date of shipment or for five years after the agents are consumed or properly disposed, whichever is longer. *See* 42 C.F.R. § 72.6(d)(3) (1999).

exposure of laboratory workers, other persons, and the outside environment to potentially hazardous agents. Containment is divided into two categories: primary (safety equipment)[98] and secondary (facility design).[99] Laboratory management is responsible for providing facilities commensurate with the laboratory's function and the recommended biosafety level for the agents.[100]

b. Transfer Regulations

Transfers of biological agents must be tightly regulated because of the disastrous consequences of an accident resulting in release or theft of agents for illegitimate purposes. Therefore, before shipping of any select agent, the transferor and the requestor must complete forms that require information about the requestor and transferor, the names of the facilities, the agents, the number and amount of containers of agents, and the names of those responsible. During the shipping process, the agents or products must be labeled, shipped, and packaged according to federal regulations. The packaging must be able to withstand leakage of contents, shocks, pressure changes, and other conditions incident to ordinary handling in transportation.[101]

---

98. Primary containment refers to the protection of personnel and the laboratory environment from exposure to infectious agents. *See* BMDL, *supra* note 86, at 8. Primary barriers include biological safety cabinets, enclosed containers, and other engineering controls to remove or minimize exposures to hazardous biological materials. *See id.* at 9. Safety equipment includes personal protection items such as gloves, coats, gown, shoe covers, boots, respirators, face shields, safety glasses, or goggles. *See id.* at 10.

99. Secondary containment refers to the protection of the environment external to the laboratory from exposure to infectious materials. *See id.* at 8. Recommended secondary barriers depend on the risk of transmission of specific agents. For instance, low level labs should have sinks available, and windows should be fitted for fly screens. Higher-level labs should control access to the laboratory, and special ventilation systems may be installed. *See id.* at 11.

100. *See id.* at 8-9, 14. Each laboratory should develop or adopt an operations manual which identifies the hazards that will or may be encountered and specifies practices and procedures to minimize or eliminate risks. Laboratory personnel, safety practices, and techniques must be supplemented by appropriate safety equipment, management practices, and facility design and engineering features. *See id.* at 8-9.

101. Additional requirements for handling toxins are found in *Occupational Exposure to Hazardous Chemicals in Laboratories*, 29 C.F.R. § 1910.1450 (1999). These regulations correspond with the packaging and shipping requirements for hazardous substances in 49 C.F.R. § 173 (1999). In addition, voluntary safety procedures described in the *Biosafety Manual* have been incorporated by reference in 42 C.F.R. § 72.6(a)(5) (1999).

If an accident or theft occurs during transfer of biological agents, it must be reported immediately. To facilitate tracking in the event of a lost or stolen agent, two forms are maintained, one by each party, and an additional form is sent to a central repository that can be available to federal and local enforcement authorities. Once the agent is sent, a responsible facility official who is a safety officer or a senior management official of the facility requesting such agent(s) must verify receipt. To ensure the agents have been legitimately received, this official is not to be the same person who actually transfers and receives the agent. It is the officer's responsibility to authorize receipt, as well as to verify the legitimacy of the facility and use of the agent.

These regulations are designed to protect the public against an accident or perhaps even against theft in connection with a normal robbery; they are not designed to protect against a deliberate effort by well-organized terrorists to obtain pathogens for the purpose of propagation. As stated earlier, this is not a likely route for a terrorist to pursue because the theft would alert law enforcement authorities. Yet it may be reasonable to consider to what extent it would be appropriate to apply to transfers of pathogens the far more detailed requirements that apply to transfers of nuclear materials.[102] Second, under current law, improper containment or labeling of pathogens in transit is not a criminal offense (barring evidence of a willful disregard of public health and safety). It may be appropriate to consider in this connection the merits of attaching criminal penalties to improper transfers of pathogens regardless of the offender's intent.

c. Personnel Regulations

Because small samples of biological agents can be propagated, anyone with access to the agents could create a weapon from just a single vial. Therefore, persons working with select agents or who have access to the agents through their affiliation with the facility (such as janitors and security) are subject to regulations restricting their access.[103] Only people

102. 10 C.F.R. §§ 110.1-110.9.

103. *See Assessing the Adequacy of Federal Law Relating to Dangerous Biological Agents: Hearing Before the House Commerce Comm.*, 106th Cong. (1999) (statement of Nancy D. Connell) ("[I]ndividuals with access to these agents may well be the first

who are actually concerned with propagation of the culture, production of the vaccine, and unit maintenance are allowed in areas that process live vaccines.[104]

Personnel inside a facility may pose a significant threat of diversion, justifying implementation of personnel requirements similar to those in the nuclear industry, including background checks and psychological testing.[105] These measures, however, raise significant privacy concerns both as to how information is gathered as well as to how it is distributed to relevant government agencies and, perhaps, private entities. Confidentiality measures may be appropriate for information obtained through checks and testing.

The security interests at stake in personnel profiling will likely overcome an employee's right to privacy. In *McKenna v. Fargo*,[106] employment was conditioned on taking tests that included questions on religious beliefs, political opinions, and familial relationships.[107] The district court held that the right to privacy extends to employer-mandated psychological testing because of the disclosure of highly personal information, but upheld the public employer's testing.[108]

4. *Stopping Importation of Pathogens*

Bringing biological agents into the United States for sale, barter, or exchange is prohibited unless the importer holds a permit for the product.[109] Each package of imported biological products must be properly packaged and labeled or plainly

---

link in the scenario we are trying to prevent from occurring: inappropriate transfer/possession of a listed agent. . . . On occasions when individual possession (i.e. by a worker) is necessary, that individual should be authorized in writing by the registered facilities sending and receiving the agent.").

104. *See* 21 C.F.R. § 600.10(b) (2000) (requiring personnel to have capabilities commensurate with their assigned functions, a thorough understanding of the manufacturing operations, necessary training and experience relating to individual products, and adequate information concerning applicable regulations).

105. Current regulations do not require background checks, psychological testing, or clearance procedures.

106. 451 F. Supp. 1355 (D.N.J. 1978).

107. *See id.* at 1377.

108. *See id.* at 1382 ("[T]he intrusion on plaintiffs' constitutionally based privacy interests was justified by the State's need for a procedure which advanced compelling State interests and which was narrowly drawn to further only those interests.").

109. *See* 42 C.F.R. § 71.54(a) (1999) ("A person may not import into the United States, nor distribute after importation, any etiological agent . . . or vector of human disease . . . unless accompanied by a permit issued by the Director.").

marked,[110] and it may be subject to random sampling by customs officials.[111] If a biological product is unlicensed, it will be detained until a proper permit is obtained.[112] Unfortunately, biological agents are difficult for customs to detect. Unlike guns, grenades, and plastic explosives, biological agents cannot be detected by x-ray machines, trained dogs, metal detectors, or neutron bombardment.[113]

To have any realistic chance of detecting clandestine imports of pathogens, new tagging and tracking technologies that can monitor the flow of products through ports are needed to supplement time-consuming and altogether inefficient border examinations by government inspectors. Although the legal issues associated with remote sensing capabilities which are discussed below are not particularly salient in regard to customs controls, effective use of new monitoring technologies will require international cooperation on an unprecedented scale. In brief, multilateral agreements will be needed to compel transporters to maintain and provide access to supply-chain information that can assist inspectors at borders.[114]

B. Regulation of Biological Weaponization Equipment

Strong security measures significantly diminish the risk that terrorists will obtain pathogens from laboratories, pharmaceutical companies, or other legitimate sources. Even the strongest security measures to prevent terrorists from gaining access to pathogens could be overcome, but the probability of failure is very high and success would tend to arouse a relentless investigation. More likely, a terrorist would obtain pathogens either from domestic natural sources or import them from outside the United States. Neither of these routes raises a troubling risk of discovery for a potential terrorist, and there is not much that legal measures, even in an ideal context, could do to render discovery likely.

Fortunately, this frightening portrayal is incomplete. In order to engender mass casualties, pathogens from natural sources

110. *See* 42 C.F.R. § 72.3 (1999).
111. *See* 42 C.F.R. § 72.6(g) (1999).
112. *See* 42 C.F.R. § 71.54(b) (1999).
113. *See* Purver, *supra* note 2.
114. *See* Stephen E. Flynn, *Beyond Border Control*, FOREIGN AFFAIRS, Vol. 79, No. 6, Nov-Dec. 2000, at 57-68.

must be weaponized, a sophisticated process usually requiring advanced equipment and a highly developed laboratory. A terrorist-importer is not likely to carry weaponized agents but would instead smuggle unprocessed agents from abroad, perhaps in freeze-dried form, and weaponize them domestically. Weaponization, therefore, is the critical junction where regulatory efforts might be effective.

Regulation of equipment used for simple fermentation or small scale weaponization would not be practicable because much of the equipment is commonplace. As discussed above, cultivating a large quantity of pathogen from a small seed culture is trivial, requiring little more than common equipment, agar, and a fermenter similar to that used for homemade beer. None of this equipment could reasonably be regulated, nor would any regulatory system divert or deter the production of biological weaponry. Any regulation would require burdensome recording by the private sector, especially pharmaceutical firms and related companies. Weaponizing pathogens for purposes of attacking an individual or a small group requires more expertise than propagating the agent, but the necessary equipment is widely available and difficult to effectively regulate. By contrast, weaponizing pathogens for a mass attack having catastrophic consequences is, as explained in Part I, a far more difficult undertaking.

1. Functions of Critical Weaponization Equipment

Sophisticated equipment is necessary to enable a terrorist with respectable but not extraordinary skills in manipulating pathogens to fashion particles small enough to: (1) disperse broadly over the relevant target population; (2) be retained by the target when contact is made; and (3) stay viable for a prolonged period so that a large portion of the target population will be infected. Such equipment allows terrorists to decrease particle size without killing off the agent. Complex fermentation and large scale weaponization equipment sufficiently sophisticated for inflicting catastrophe can be regulated efficiently and without undue burden.

The bioterrorist's need for critical biological equipment led the Australia Group to call on member States to restrict exports of seven categories of dual-use equipment relevant to biological weapons: (1) complete containment facilities at P3 and P4

containment levels; (2) fermenters; (3) centrifugal separators; (4) cross-flow filtration equipment; (5) freeze-drying equipment; (6) equipment that incorporates or is contained in P3 or P4 containment housings; and (7) aerosol inhalation chambers.[115] The U.S. Bureau of Export Administration has promulgated a functionally similar list of restricted items and will deny a license application if the export could be destined for the design, development, production, or use of missiles or chemical or biological weapons, or for a facility engaged in such activities.[116]

Fermentation equipment is used to grow and harvest biological agents. Although simple fermentation equipment such as that used for brewing beer may be suitable to grow some microorganisms, it is not efficient for the most pathogenic microorganisms and may be inadequate for weaponization. Organisms such as *bacillus anthracis* could not be easily grown in basic fermentation vessels, and separating the spores from the media would be very difficult. Viruses are also not easily grown and extracted in such equipment. Sophisticated fermentation equipment—necessary to control atmospheric, temperature, and chemical parameters—supports efficient microorganism growth, facilitates harvesting, and permits near-continuous production. For these reasons, fermentation equipment is most relevant to export or other controls.

Centrifugal Separators separate materials based on relative density in order to concentrate solutions, separate viruses from bacterial hosts, and separate microorganisms from media. Temperature control in differential centrifugation is important, particularly when separating viruses that are very heat sensitive. Temperature-controlled, high-speed, differential

115. *See* Australia Group, Biological Weapons: List of Dual-Use Biological Equipment for Export Control, *at* http://dosfan.lib.uic.edu/acda/factshee/wmd/bw/auslist.htm (Nov. 7, 1995).

116. *See* Cecil Hunt, *The Export Licensing System*, *in* COPING WITH U.S. EXPORT CONTROLS 25, 49-50 (PLI Commercial Law and Practice Course Handbook Series 1993); *see also* Chemical and Biological Weapons Control and Warfare Elimination Act of 1991, 22 U.S.C. §§ 2798, 5601-06 (2000); Australia Group, List of Biological Agents for Export Control Core List, *at* http://projects.sipri.se/cbw/research/AG-bw-bwagents.html (last modified Aug. 18, 1998). The Federation of American Scientists has addressed triggers for aerosol equipment and has recommended a compliance regime based on transfers and acquisitions of listed priority pathogens and equipment. *See* Federation of American Scientists Working Group on BW Verification, Aerosol Trigger, *at* http://www.fas.org/bwc/papers/aer2.htm (Dec. 1998).

centrifuges are therefore most relevant to export controls. Smaller desktop centrifuges would be inefficient and lack the speed and temperature control to effectively separate viruses.

Cross-flow filtration equipment is used to maintain suitable growth conditions in the fermentation vessels as well as to separate microorganisms from media. Unlike a differential centrifuge, this equipment is not commonly found in general research labs.

Freeze-drying equipment is particularly important to preserve the condition of spores and would be particularly important in freeze-drying anthrax spores with a substrate that can easily be dispersed in the environment. Freeze-drying equipment is not something that is commonly found in a general research lab, but is widespread in commercial applications.

Aerosol inhalation chambers are lower-pressure, higher-temperature concentration vessels into which liquid is pumped. This process results in expansion of the liquid into a near-vapor state permitting concentration of the agent.

While there are export controls applicable to critical biological weapons equipment, there are not, at this time, regulatory controls on domestic transfers. The degree to which this fact is significant to biological weapons production evokes the incessantly and inconclusively debated question of how easy or difficult is it to make biological weapons. The more dependent that biological weapons production is on critical equipment, the more reasonable it is to regulate that equipment. By contrast, if biological weapons production requires only off-the-shelf equipment or is so difficult that even access to the best equipment poses no risk, then regulation of critical biological equipment is a waste of time and money. A more profitable discussion should focus on alternatives for action.

2. *Optional Recommendations*

a. *Domestic Market*

The following recommendations are intended to apply to *critical equipment*, equipment crucial to the effective operation of a catastrophic biological weapons program and having narrow or specialized commercial uses such that controls are

likely to be efficiently implemented. They are arranged in increasing order of intrusiveness and burdensomeness. The recommendations are not mutually exclusive.

i. Voluntary Know-Your-Customer Guidelines

Sellers of critical equipment could be obligated to know to whom they are selling that equipment and the purpose for which that equipment will be used. At a minimum, this requirement could be implemented as a recognized industry practice (i.e., without government oversight or enforcement).

ii. Tagging Capabilities

Each item of critical equipment could be fitted with a signal emitter that would enable law enforcement or regulatory officials to determine its location.[117] Removal of that signal could be made technically impossible or could be grounds for imposing liability. Virtues of this recommendation include low expense and minimal regulatory burden.

iii. Enforceable Know-Your-Customer Guidelines

Sellers could be liable if they sell equipment to persons whom they have reason to doubt will put that equipment to legitimate use. This option carries no regulatory burdens but could deter sales to potential terrorists by threat of subsequent imposition of penalties. Sellers could have a duty to check out "red flags."[118] Red flags include orders for items that are inconsistent with the needs of the purchaser, a customer declining installations and testing when included in the sales price or when normally requested, or requests for equipment configurations that are incompatible with the stated destination.

Sellers who proceed with a transaction in the face of unexplained or unjustified "red flags" run the risk of being

117. *See generally* Barry Kellman & David S. Gualtieri, *Barricading the Nuclear Window: A Legal Regime to Curtail Nuclear Smuggling*, 1996 U. ILL. L. REV. 667 (1996); WOLFGANG H. REINICKE, GLOBAL PUBLIC POLICY: GOVERNING WITHOUT GOVERNMENT? 207-08 (1998); *Tags*, Lawrence Livermore Nat'l Lab., http://www.llnl.gov/eng/ee/erd/isq/tags.html; *Technology Breakthroughs: Small and Mighty . . . It's All in the Tag*, BREAKTHROUGHS MAG., Pacific Nat'l Lab., Spring 1999, http://www.pnl.gov/breakthroughs/spring99/techbreaks.html.

118. *See* COPING WITH U.S. EXPORT CONTROLS 864 (PLI Commercial Law and Practice Course Handbook Series 1993).

attributed the "knowledge" required to make the action illegal. It is worth noting three subsidiary issues: First, is receipt of bad information or the buyer's concealment of material facts an excuse from liability, and if so, are affirmative steps to avoid bad information a mitigating factor? Second, is failure to take steps to investigate the buyer an aggravating factor to be considered in an enforcement proceeding? Third, is the seller obligated to obtain documentary evidence concerning the buyer's use?

iv. Declaration of Transfers

Sellers could be obligated to document with a relevant government agency any transfer or acquisition of critical equipment to a domestic or foreign purchaser. Provisions would have to be implemented to maintain the confidentiality of declared information. Documented information could include the equipment's source and destination, the approximate quantity, its intended use, and information on unfilled transfer requests.

v. Certification or Licensing of Purchasers

Existing regulations require that pathogens may be sold only to purchasers certified to have access to them. Every possessor must retain a license recorded in a database (available to federal authorities and industry members). Similar regulations could be applied to critical equipment. Accordingly, sellers could check the database for licensed possessors. A new licensee would be subject to required federal background checks and a waiting period. Violators of specific provisions would be decertified and therefore prohibited from gaining access to critical equipment.

b. Export Market

Export controls prohibit export licenses for items that could be destined for the design, development, production, or use of biological weapons if they would be detrimental to national security.[119] Factors considered in this determination include the nature of the end use, the significance of the export to the

119. 15 C.F.R. § 742.2(b)(1).

prohibited use, the non-proliferation credentials of the importing country, and the assurances against misuse of the item.[120] Concerns have been expressed as to the risk of resale or retransfer.[121] To diminish the risk of resale or retransfer, additional factors could be considered in the license application process, including the controls the importing country exerts over the items after their import, whether the export laws of the importing country serve to minimize the risk of resale or retransfer, whether such laws are adequately enforced, and the importing country's participation in various multinational systems to prevent proliferation of weapons of mass destruction.

III. LAW ENFORCEMENT TO COMBAT BIO-TERRORISM

Preventing access to pathogens and critical equipment can diminish risks of bioterrorism, but it would be foolhardy to believe that the regulatory measures previously discussed can eliminate the threat. Pathogens can be imported or cultivated from natural sources, and equipment to propagate those pathogens is widely available. Production of deadly devices is difficult, but domestic or foreign terrorists will be capable of overcoming technical obstacles. Rigorous law enforcement measures must address the threats of bioterrorism; the question is how?

Much of the law enforcement effort is standard; conventional surveillance and investigatory techniques apply to bioterrorism just as they would to more commonplace criminal activity. Arguably, beneficial initiatives could include increasing technological and personnel resources and streamlining cooperation between federal and local law enforcement authorities. But it would be wrong to contend that the current law enforcement effort is insubstantial.[122] While it stands to

120. 15 C.F.R. § 742.2(b)(2).

121. *See* Barry Kellman, *Bridling the International Trade of Catastrophic Weaponry*, 43 AM. U. L. REV. 755 (1994); Gary Milhollin, *Stopping the Indian Bomb*, 81 AM. J. INT'L L. 593 (1987); Jeffrey L. Snyder, *International Operations: Managing the Risks*, N.Y. L.J., May 20, 1996, at S4.

122. *See* HOUSE PERMANENT SELECT COMM. ON INTELLIGENCE, 104TH CONG., IC21: INTELLIGENCE COMMUNITY IN THE 21ST CENTURY ch. XIII (1996).

> Recent claims that the FBI is hamstrung in its efforts to combat domestic terrorism are incorrect. In any given year, the FBI engages in approximately two dozen full domestic terrorism investigations. Nearly

reason that more resources for law enforcement would help to combat bioterrorism, this Part does not grouse about current efforts.

That said, two characteristics distinguish biological terrorism from other crimes. First, the mechanism of the crime is essentially undetectable once it is deployed. Second, the crime has altogether unacceptable consequences. These characteristics mean that post-event law enforcement is of limited value; techniques must be employed before the crime to protect society from decimation. The need to empower law enforcement capabilities *before* the commission of a crime raises issues unique to the threat of biological terrorism that do not fit within typical law enforcement parameters.

This Part discusses four issues. First, is conduct relevant to bioterrorism sufficiently covered by federal criminal law; if not, what modifications should be enacted? Second, what information should be sufficient to stimulate an initial inquiry into the activities of suspected bioterrorists, and how can traditional law enforcement mechanisms of information-gathering be supplemented in order to improve bioterrorism prevention? Third, what are the appropriate uses of biosensors and how can their increased use be reconciled with privacy considerations? Fourth, when threats of emergency arise, how should the power law enforcement has to conduct extraordinary searches and related measures be evaluated in light of the Fourth Amendment and other constitutional strictures?

Underlying the discussion of these issues is a commitment to a meticulous approach to the juncture between law enforcement measures that might be necessary to prevent bioterrorism and a healthy respect for civil liberties. Biological terrorism poses an unprecedented challenge to America's commitments to liberty and justice. Its objective is to demonstrate that, under stress, these commitments are frail and shallow. Thus, terrorism's ultimate target is the Constitution, and its greatest victory would be to see this nation undermine civil liberties in the name of reacting to terrorism. The ends of security from terrorism do not justify means which abrade the

---

two-thirds of these full investigations are opened before a crime has been committed in order to prevent terrorist crimes before they occur.

Id.

principle that the government derives authority from the rule of law. Indeed, it erodes the foundations of liberty to contend that because terrorists reject legal restraints, adherence to the Bill of Rights should be abdicated in the cause of national security.

The Constitution permits law enforcement officials to perform functions necessary to protect the public safety and preserve order so long as those functions are anticipated and carried out in a manner that is reasonably proportional to a legitimate government interest such as public health, investigation of crimes, or national security.[123] There is no substantial evidence that law enforcement measures in contravention of constitutional rights might actually be effective against terrorism. Nor have experts identified legal inhibitions, restrictions, or prohibitions on law enforcement authority that are applicable in normal circumstances which should be abandoned, mitigated, or suspended in the highly unusual circumstances of counter-terrorism. To the contrary, counter-terrorism measures that unreasonably truncate rights of privacy and due process of law are unwarranted and offensive.

A. Criminalizing Bio-terrorism

It is a crime, of course, to create, transfer, or possess pathogens or their delivery systems for use as a weapon[124] unless the accused demonstrates that the development or possession of agents was "for a prophylactic, protective, or other peaceful purpose."[125] Moreover, the prohibition against use of weapons of mass destruction specifically includes weapons involving disease organisms as well as genetically altered products,[126] punishable by up to life imprisonment or, if

123. *See* National Treasury Employees Union v. Von Rabb, 489 U.S. 656 (1989) (upholding suspicionless drug testing of customs officials); *cf.* New Jersey v. T.L.O., 469 U.S. 325 (1985) (upholding search of student's purse). *See also* Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen*, 94 COLUM. L. REV. 1751 (1994).

124. 18 U.S.C. § 175(a) (2000).

125. 18 U.S.C. § 177(b)(1) (2000).

126. *See* 18 U.S.C. § 2332a (2000) (prohibiting any use, threat, attempt, or conspiracy to use a weapon of mass destruction, including any biological agent, toxin, or vector).

death results, the death penalty.[127] It is unclear whether a hoax constitutes a threat within the meaning of this section.

These prohibitions, applicable in response to a bioterrorist event that may have catastrophic consequences, have limited value. To protect society, rigorous law enforcement techniques must be employed before the bioterrorist crime is committed. Faced with an unaccomplished crime, prosecutors have potential problems in producing evidence to prove a defendant possessed deadly agents for use as a weapon, not for a legally acceptable purpose. Indeed, this hurdle impeded prosecution of Larry Wayne Harris, discussed above, because he claimed that his possession of pathogens was legally protected.[128] The implication here is that someone can legally possess a pathogen without a license, and that it is up to the prosecution to prove intent with evidence other than mere possession. Thus, even someone with acknowledged scientific training in handling and processing pathogens and with a record of anti-social and perhaps criminal conduct can legally possess pathogens and may do so covertly.

It would be preferable simply to prohibit knowing possession of pathogens without a license, simplifying the task of prosecution. Because only licensed facilities could legally develop or possess pathogens, this change would reinforce the primacy of the licensing system by making the regulatory process the proper venue to determine the applicant's purpose and intent; necessarily, any possessor of pathogens who does not successfully obtain a license is subject to prosecution and, at minimum, would face penalties for noncompliance with regulatory reporting requirements. Most important, with a straightforward prohibition against unlicensed possession, law enforcement officials would not have to wait to apprehend the suspect until he demonstrates an intent to use pathogens as a weapon. Someone found to have cultivated pathogens but who has not registered with the CDC or who has submitted false information concerning her activities could be arrested. For these reasons, the Department of Justice has championed making it a federal crime to possess weaponizable agents

127. *See* 18 U.S.C. § 2332a(a)-(b) (2000).

128. *See* Stern, *supra* note 82, at 227. Harris pled guilty to mail fraud. *See id.*

without regulatory approval.[129]

B. Gathering Information and the Detection of Clandestine Bio-terrorism

Undeniably, the best security against biological terrorism is the ability to obtain information about potentially catastrophic activities sufficiently in advance of an attack to be able to prevent it.[130] Just as undeniably, law enforcement officials cannot track every conceivable possibility both because of finite resources and because of civil liberties protections that enable Americans to avoid constant surveillance. It is facile to say that priorities must be set; the important question is what activity should provoke a pre-attack investigation. This Section suggests that, in limited respects, the FBI and their state and local counterparts may be looking in the wrong places and asking the wrong questions.

Counter-terrorism law (which guides application of law enforcement resources) is based on a 1970s conception of terrorism that identifies terrorist activity with groups that have distinct ideological commitments and use terrorism to gain attention to their cause. Revolutionary terrorists, aspiring to overthrow perceived repression, were characterized as seeking to achieve international recognition through overt, stunning events that would mobilize their adherents and coerce their targets into paying attention to their claims. Accordingly, the Secretary of State can designate an organization as a "foreign terrorist organization" upon a showing that the organization is foreign, "the organization engages in terrorist activity," and the terrorist activity of the foreign organization "threatens the security of United States nationals or the national security of the United States."[131] Once a foreign terrorist organization has been designated, it becomes a crime to provide "material support" to it.[132]

---

129. *See* President William Jefferson Clinton, Remarks by the President at 21st Century Crime Bill Unveiling (May 12, 1999), *available at* http://www.clinton.nara.gov/.

130. The Attorney General has authority to search for and seize pathogens that are illegally possessed; action may be taken without a warrant in an emergency. *See* 18 U.S.C. § 176 (2000).

131. 8 U.S.C. § 1189(a)(1) (2000). "Terrorist activity" is defined in 8 U.S.C. § 1182(a)(3)(B)(ii) (2000).

132. 8 U.S.C. § 1182(a)(3)(B)(iii) (2000) (defining and prohibiting material

This perception applied neatly to Hamas, the Irish Republic Army, the Red Brigade, and other prominent terrorist organizations, but terrorists like Ted Kaczynski, Tim McVeigh, and the Aum Shinrikyo group manifest quite different behavior. As discussed above, bioterrorists are likely to be more interested in spreading panic than in advancing a radical political ideology. Even if bioterrorists are sent into this country on behalf of a foreign power, only an absolute fool would employ designated members of a foreign terrorist organization. Indeed, for purposes of initiating an investigation into potential bioterrorism, criteria of suspicion must be formulated for which radical ideology is not central.

It would be more effective to base suspicion on capability rather than ideology. The amount and type of evidence sufficient to constitute a "reasonable suspicion" to investigate in advance of a bioterrorist attack relates to the definition of bioterrorism and whether unlicensed possession of pathogens is a crime. If possession is criminalized, evidence of access to biological agents, expertise in handling and processing those agents, or experience in biological research may be relevant in determining reasonable suspicion. Accordingly, unlicensed acquisition of equipment that would be useful to weaponizing biological agents should prompt an inquiry as to the purposes for that equipment, as part of the system of monitoring domestic transfers of biocritical equipment advocated in Part II.

Perhaps the most useful allocation of law enforcement resources would be to monitor hate groups, especially those that have declared an interest in pathogens. It is currently illegal to teach or demonstrate to any person any "technique capable of causing injury or death to persons, knowing or having reason to know or intending that the same will be unlawfully employed for use in, or in furtherance of, a civil disorder . . . ."[133] There are recurrent proposals to prohibit distribution of information relevant to a destructive device with the intent that the information will be used, or knowledge that it will be used, for or in furtherance of an activity that constitutes a federal crime of violence.[134]

Three noteworthy issues arise from these prohibitions. First,

support).

133. 18 U.S.C. §231(a)(1) (2000).

134. *See* 21st Century Justice Act, S. 899, 106th Cong. (1999).

restricting the dissemination of information has obvious First Amendment implications. Second, assuming these restrictions are constitutional, it is difficult to determine whether a person disseminating relevant bioterrorism information has the intent or knowledge that it will be used to create a civil disorder or in an activity that constitutes a violent crime. Third, in view of the fact that Internet sites can easily be located outside the jurisdiction of U.S. law, it is difficult to conceive of how even the most determined effort could prohibit bioterrorists from exchanging information.

It may be appropriate to consider the constitutionality and law enforcement efficacy of prescribing that dissemination of information relevant to bioterrorism will constitute reasonable suspicion to justify investigation and even intrusive surveillance methods. Terrorist web pages, pages discussing biological terrorism, as well as hate group, militia, and other radical information on the Internet could be used to initiate or direct investigations. This proposal somewhat mitigates the First Amendment implications of a prohibition on dissemination (speech would be chilled but not prohibited). However, the proposal also raises Fourth Amendment concerns about the quantity and quality of evidence sufficient to undertake various law enforcement search methods. A related approach is to charge persons disseminating bioterrorism information with aiding and abetting a criminal use or attempt.

C. Use of Biosensors

Pathogens are not visually detectable, nor do they send obvious signals comparable to the radiation emitted by nuclear materials. Real-time detection and measurement of biological agents in the environment is further complicated by the number of potential agents to be distinguished, the complex nature of the agents themselves, the myriad of similar microorganisms that are a constant and natural presence in the environment, and the minute quantities of pathogen that can initiate infection. Thus, pre-attack detection of weaponization facilities or transport of pathogens is extremely difficult. Even after a bioterrorist attack, there is little that can be done to trace the movement of pathogens or to identify their dissemination. Technologies capable of detecting the presence of pathogens

obviously would be a powerful asset to law-enforcement officials.

Biosensors are miniature devices that convert information about biological material in the environment into an electrical form that can be read by instruments. They have at least three distinct applications that are directly relevant to preventing bioterrorism:[135] (1) to protect air distribution systems; (2) to identify pathogens on persons passing through a portal; and (3) to monitor facilities in order to detect clandestine bioweapons production. These applications of biosensors do not constrain or physically intrude on a person's liberty; furthermore, sensors tend to be exceptionally selective, i.e., they do not uncover broad categories of information in excess of what law enforcement requires. Yet widespread use of biosensors (not technically realistic today but a potential for the near future) should be carefully considered in light of the implications of such use for privacy.

1. Protection of Air Distribution Systems

Sensors could be used to detect the presence of biological agents in air distribution systems where they might be placed by a terrorist intending to harm persons who rely on those distribution systems. In this context, sensors would be entirely passive, lying in wait and functioning analogous to smoke alarms; when stimulated by the presence of certain pathogens, they would either set off a warning or, preferably, shut down the air distribution system. These types of sensors could offer significant protective capabilities but would be essentially irrelevant to law enforcement efforts to detect and stop terrorists, and their use raises no significant legal questions. If such sensors are technologically and economically feasible, they could serve an extremely useful function for some

135. Bio-sensing technology is crucially important in detecting and identifying pathogens in clinical samples. Technologies relevant to this function are advancing rapidly, far beyond the scope of this discussion. Although there are privacy issues attendant to the use of laboratory diagnostics, especially in cases where a sample has been taken from a person without overt consent, those issues are unrelated to the privacy concerns relevant to prevention of bioterrorist attacks and, therefore, are not discussed further. *See, e.g.*, Guido S. Weber, *Unresolved Issues in Controlling the Tuberculosis Epidemic Among the Foreign-Born in the United States*, 22 AM. J. L. & MED. 503 (1996); Andrew S. Krulwich & Bruce L. McDonald, *Evolving Constitutional Privacy Doctrines Affecting Healthcare Enterprises*, 55 FOOD & DRUG L.J. 491 (2000).

facilities, such as enclosed stadia where thousands of people rely on the same air source.

2. *Checkpoint Detectors*

Sensors could be used to detect the presence of trace amounts of pathogens on persons who pass through a portal or checkpoint. These biosensors could perhaps be used at airport checkpoints, in tandem with current metal-detection capabilities. Because pathogens portend less immediate yet more widespread violence than guns, these portal-based sensors would be better used to check disembarking persons. Indeed, this application, if technologically effective, would be virtually the only way to defend against importation of foreign pathogens.

The constitutionality of portal-based sensors is supported by the use of airport checkpoints, which has long been upheld in view of the significant threat of hijacking and bombing to public safety and security.[136] This logic might justify the legality of using portal-based biosensors. However, other modern technologies analagous to biosensors have been criticized. Mechanical canines "sniff" around a person to detect the presence of narcotics. A device named Sentor uses portable vapor phase chromatography to analyze particles on and around individuals.[137] The courts have not yet ruled on the constitutionality of these devices. Concerns have been raised that with these types of sensors—which only detect the presence, but not the source, of contraband in the air—innocent persons may be wrongfully accused or detained.[138] A similar

136. *See, e.g.*, United States v. Doe, 61 F.3d 107, 109-10 (1st Cir. 1995) (stating that "routine security searches at airport checkpoints pass constitutional muster because the compelling public interest in curbing air piracy generally outweighs their limited intrusiveness"); United States v. De Los Santos Ferrer, 999 F.2d 7, 9 (1st Cir.) (describing airport searches as administrative searches conducted for a "limited—and exigent—purpose"), *cert. denied*, 510 U.S. 997 (1993); United States v. $124,570 U.S. Currency, 873 F.2d 1240, 1243-47 (9th Cir. 1989) (describing airport security searches as narrowly limited to their compelling administrative objective of searching for weapons and explosives).

137. *See* Richard S. Julie, Note *High-Tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age*, 37 AM. CRIM. L. REV. 127 (2000); Jason Lazarus, Note, *Vision Impossible? Imaging Devices—The New Police Technology & the Fourth Amendment*, 48 FLA. L. REV. 299 (1996).

138. *See* Peter Joseph Bober, *The "Chemical Signature" of the Fourth Amendment: Gas Chromatography/Mass Spectrometry and the War on Drugs*, 8 SETON HALL CONST. L.J. 75, 108-117 (1997).

objection could be made in regard to bioweapons-sensing technologies.

The analogy to metal detectors is potentially inapt because biosensors reveal information that is potentially more sensitive than what is revealed when one passes through a metal detector. While it is difficult to conceive of how a person could have an intimate privacy interest in metal on one's body, detection of biological substances could reveal the presence of a socially-despised disease or condition, thereby subjecting a person to embarrassment or worse. Even the prospect of having intimate details of one's physiology checked over might be considered offensive regardless of whether there are consequences to that check. Canine sniffers, too, likely provide an inapt analogy. A person's privacy interest in illicit narcotics on his body (if it exists at all) is decidedly less than a person's privacy interests in the intimate details of his own physiology. Ongoing controversies surrounding Millivision and related sensory-enhancing technologies[139] may present better points of reference. The Millivision detectors register the millimeter waves naturally emitted from the human body, enabling an operator to get a fairly detailed outline of a person's body; if the person is carrying a gun, it would show up as an anomaly.[140] As capabilities improve, "a point may be reached where the information provided to the operator about the person's body is of such a personal character that the intrusion is no longer justified—even by the heightened government interest."[141]

3. *Emissions Detection*

By far the most important use of biosensors would be to detect the presence of biological laboratories by analyzing air emissions from those facilities. As discussed above, the most likely bioterrorist strategy involves obtaining a pathogen from an undetectable natural or foreign source and weaponizing that

139. *See* T. Wade McKnight, Comment, *Passive, Sensory-Enhanced Searches: Shifting the Fourth Amendment "Reasonableness" Burden*, 59 LA. L. REV. 1243, 1265 (1999).

140. *See id.*

141. *Id.*; *see also* Steven Salvador Flores, Note, *Gun Detector Technology and the Special Needs Exception*, 25 RUTGERS COMPUTER & TECH. L.J. 135 (1999); Alyson L. Rosenberg, Note, *Passive Millimeter Wave Imaging: A New Weapon in the Fight Against Crime or a Fourth Amendment Violation?* 9 ALB. L.J. SCI. & TECH. 135, 159 (1998).

pathogen at a clandestine laboratory. A method to detect that laboratory would thus serve a crucial prevention function. This application is analogous to environmental sampling for pollution emissions from industrial sites. Such sensors would enable law enforcement officials to collect information otherwise unavailable without any physical intrusion. The suspect would normally not even be aware of the surveillance because the device "passively" measures the natural emissions from the target.

A practical detection system would have to discriminate between closely related organisms because many pathogens differ little from normal microorganisms. New technology can take advantage of the high affinity and specificity that a pathogen has for its natural receptor.[142] Natural cell receptors for viral pathogens can be used in a biosensor to selectively and sensitively identify the pathogen in a biological warfare agent.

This system will face significant technical hurdles, however. Any closed system capable of containing emissions would escape detection. Even if pathogens are emitted, the sensor would need to distinguish biological weapons agents from normal microorganisms. The sensor would therefore need to be extremely selective. Moreover, this type of sensor can only detect a pathogen it is programmed to detect; terrorist use of another pathogen or a genetically modified pathogen would likely go undetected precisely because a practically useful sensor must not respond to every pathogen in the environment.

"Few, if any, civilian agencies at any level currently have even a rudimentary capability in this area. A number of military units, most notably the Army's Technical Escort Unit, the U.S. Marine Corps Chemical Biological Incident Response Force, and the Army Chemical Corps, presently have some first-generation technology available."[143] The need for faster,

142. Pathogenic bacteria possess novel proteins designed to help them overcome normal host defense mechanisms. Recently, there has been a virtual explosion of information identifying bacterial factors that are needed as accessories to transport virulence factors to the cell surface where they can be detected. *See, e.g.*, Defense Advanced Research Project Agency, Biological Warfare Defense Sensors, *at* http://www.darpa.mil/spo/programs/biowarfaredefensesensors.htm (announcing and describing new program to develop biological warfare defense sensors) (last visited January 10, 2001).

143. *See* COMM. ON R&D NEEDS, *supra* note 4, at 86. For example,

> [T]he Biological Integrated Detection System (BIDS) continuously samples ambient air and determines the background distribution of

more reliable detection of hazardous biological agents has spawned a large and growing number of research programs.[144]

From a Fourth Amendment perspective, the use of sensors to detect emissions from facilities would not appear to raise serious problems. Sampling of air emissions by the EPA in connection with air pollution control has not been successfully challenged, although in those cases the monitored facilities were on notice of being within the scope of the Clean Air Act's regulation and therefore had a diminished expectation of privacy as to their emissions.[145] Greater legal controversy has attended the use of thermal imaging devices used to detect differences in temperature on the surface of a selected target.[146] Current thermal imagers are capable of detecting tiny temperature differences and can locate a human in the dark from over four miles away.[147] These devices are not capable of seeing through an object but can detect heat sources that are hidden from view due to the heat that passes through the intermediate object.[148] Legal challenges to the government's use of thermal imager readings claim that use of an imager is itself a search and should not be conducted without a warrant issued on independent probable cause.[149] The United States circuit courts of appeal are split as to the constitutionality of using thermal imagers and the Supreme Court has granted certiorari to resolve that split this Term.[150]

> aerosol particles. Aerosol particles with diameters in the 2 to 10 micron range are concentrated and analyzed for biological activity . . . . [A]ntibody-based tests are conducted for specific agents. At present, the system includes tests for the bacteria responsible for anthrax, plague, botulinum toxin A, and staphylococcal enterotoxin B.

Id. at 86-87.

144. *See id.* at 78-96.

145. *See* Air Pollution Variance Bd. of Colo. v. Western Alfalfa Corp., 416 U.S. 861 (1974).

146. *See* McKnight, *supra* note 138, at 1249. *See generally* Mark D. Kiser, Comment, *Constitutional Law: Fourth Amendment Search and Seizures and Thermal Imaging*, 51 FLA. L. REV. 723 (1999) (discussing United States v. Kyllo, 140 F.3d 1249 (9th Cir. 1998)).

147. *See* McKnight, *supra* note 138, at 1249.

148. *See id.*

149. *See id.* at 1250-51.

150. *See id.* McKnight notes:

> Four circuits have approved the pre-warrant use of thermal imagers: the Fifth Circuit in *United States v. Ishmael*, [48 F.3d 850 (5th Cir. 1995),] the Seventh Circuit in *United States v. Myers*, [45 F.3d 668 (7th Cir. 1995),] the Eighth Circuit in *United States v. Pinson* [, 24 F.3d 1056 (8th Cir. 1994,] and the Eleventh Circuit in *United States v. Ford* [, 34 F.3d 992 (11th Cir. 1994),] and *United States v. Robinson* [, 62 F.3d 1325 (11th Cir. 1995)]. However,

Notably, biosensors would be less capable of detecting sensitive private information than are thermal imaging devices. For example, area-wide or environmental biosensors could not detect information that most people consider private, such as the presence of numerous people in a building, nor could they detect heat-generating equipment. Yet biosensors raise issues, analogous to the discussion above of what evidence should be required to initiate a search, concerning the basis for focusing biosensors on a particular location. If transfers of sophisticated biological equipment are tracked, as suggested above, is a building containing a regulated fermenter a legitimate target for sensor surveillance? What about a survivalist group's compound? To the extent that biosensing technologies become more prevalent, the interests at stake in their wide-scale application should be carefully weighed.

D. Emergency Authorities for Catastrophic Terrorism Situations

Identification of an imminent threat of biological terrorism, through intelligence sources or other means, should prompt the most rigorous law enforcement efforts to uncover its source and prevent the harm before it materializes.[151] Moreover, in the immediate aftermath of a terrorist event, an equivalent standard of rigor should apply to efforts to apprehend the culprits. In these biological terrorism situations, an important question arises as to whether "emergency authorities" might be necessary or advantageous for law enforcement personnel or for public health officials. Are there legal inhibitions, restrictions, or prohibitions are applicable in normal circumstances that should be abandoned, mitigated, or suspended in the circumstances of biological terrorism? If so,

---

two other circuits have issued opinions reaching different conclusions. The Tenth Circuit, in *United States v. Cusumano*, [67 F.3d 1497 (10th Cir. 1995),] ruled that the pre-warrant use of thermal imagers was unconstitutional. Then, on rehearing, the opinion was vacated because the court found independent probable cause. Later, in *United States v. Kyllo*, [140 F.3d 1249 (9th Cir. 1998),] the Ninth Circuit first ruled that the pre-warrant use of thermal imagery was an unreasonable search. Then, on rehearing, the court withdrew its original opinion and, in a 2-1 decision, held that the thermal scan was not a "search" within the meaning of the Fourth Amendment. [United States v. Kyllo, 190 F.3d 1041 (9th Cir. 1999).]

Id. at 1251. The Supreme Court granted certiorari in the *Kyllo* case. *See* Kyllo v. United States, 121 S. Ct. 29 (2000). Oral arguments were held on February 20, 2001.

151. *See* COMM. ON R&D NEEDS, *supra* note 4.

what can Congress do to expand those authorities, in view of the fact that Congress cannot legalize unconstitutional activity?

Law enforcement officials at all levels will have to conduct investigations and implement measures that exceed the standards applicable to calmer situations, measures including quarantines, cordoning off of areas, vehicle searches, compulsory medical measures, and even sweep searches through areas believed to contain terrorists. These responsibilities can be undertaken most effectively and judiciously if all levels and branches of government prepare in advance for the unique, low-probability, high-magnitude threats that terrorism poses to national security. Advance preparation is also necessary to ensure that civil liberties are not undermined in the name of reacting to terrorism. Under unprecedented conditions of mass casualties, panic may overwhelm constitutional protections. When officials are unprepared to address the threat of a biological terrorist event, the risks of an overwrought response are significant.

1. Defining the Problem

The problem here is *not* about what measures can be taken in connection with a person suspected of being a terrorist. If there is reason to suspect an individual is a terrorist, then there is no serious legal problem with conducting an investigation. If a warrant can be obtained to conduct that investigation, it should be; if exigent circumstances prevent obtaining a warrant, the requirement is conditionally excused.[152] Depending on his citizenship, the suspected terrorist may have privacy rights, and no court will condone patently unnecessary or abusive law enforcement activity. But the issues pertaining to "emergency authorities" are not, strictly speaking, relevant to what can be done in regard to a suspected terrorist.

The issues pertaining to "emergency authorities" have to do with the privacy rights of everyone who is innocent but caught in the net of the investigation for the actual terrorist. The

152. *See* United States v. Place, 462 U.S. 696, 701 (1983) ("The exigencies of the circumstances" may permit temporary seizure without warrant); *see also* Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 298-99 (1967) (holding warrantless search for suspect and weapons reasonable where exigent circumstances existed); Schmerber v. California, 384 U.S. 757, 770-71 (1966) (holding warrantless blood test for alcholo reasonable when exigent circumstances were present).

problem is that in investigating or in responding to terrorist activity, law enforcement officials may direct intrusive measures against a much broader group than the actual terrorist. It is the inability to distinguish the terrorist from all the other people in the area, or to distinguish the terrorist's locale from similar locales, that creates the potential for invasions of civil liberties.[153] The following scenarios illustrate the point:

- Intelligence strongly suggests the presence of biological weapons in a six-unit apartment building, and sensor equipment has detected emissions from that building. The difficulty is that there is no evidence as to the specific location of the biological weapons. To prevent the attack, the police will have to search each apartment. If persons in any of the five unrelated apartments deny access, the police will use force, thereby violating those persons' expectations of privacy. Yet until the police enter the apartments, they have no reason to know which apartment houses the terrorist.
- Intelligence strongly suggests that a terrorist is of a certain ethnicity, but further identifying information is unavailable. To pursue the investigation, the police will have to stop everyone who matches that characteristic. Again, the problem is not with investigating the terrorist who is of that ethnicity; the problem is that the police will have to interrogate a large number of persons who have no connection with terrorist activity.

The problem that "emergency powers" must address, therefore, is not what can be done, but rather at whom may the authorities direct their attention. It is not a question of excessive measures but a question of application of appropriate measures to an overbroad group:

> The question arises whether compulsion can be visited upon an individual simply by virtue of her inclusion in a class composed of some dangerous persons absent an individualized assessment of significant risk . . . . Perhaps the most revered principle under antidiscrimination law is the requirement to make individualized determinations of [a] person's qualifications or eligibility . . . . Given the

153. *See* Thomas K. Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV. 483 (1994).

> unequivocal requirement for individualized assessments of risk, what recourse does the state have when, despite its best efforts, it is not able to reliably separate the perceived from the truly dangerous? This becomes a formidable dilemma when the state is capable of demonstrating that the class as a whole does pose a significant health threat and where the intervention proposed is both effective and non-draconian. . . . The requirement of individualized determinations is also inherent in the doctrine of overbreadth found in the Fourth Amendment and other constitutional jurisprudence.[154]

2. *Relevant Fourth Amendment Principles*

The Fourth Amendment permits only "reasonable" searches.[155] The Supreme Court has held that the "determination of the standard of reasonableness applicable to a particular class of searches requires 'balanc[ing] the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.'"[156]

a. Applicable Doctrines

The "special needs" doctrine can justify a search, even in the absence of a warrant or probable cause.[157] "[W]here a Fourth Amendment intrusion serves special government needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion

---

154. Lawrence O. Gostin, *Tuberculosis and the Power of the State: Toward the Development of Rational Standards for the Review of Compulsory Public Health Powers*, 2 U. CHI. L. SCH. ROUNDTABLE 219, 257-59 (1995) (citations omitted).

155. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

156. O'Connor v. Ortega, 480 U.S. 709, 719 (1987) (quoting United States v. Place, 462 U.S. 696, 703 (1983)).

157. *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995). The *Vernonia* Court held:

> [A] warrant is not required to establish the reasonableness of *all* government searches; and when a warrant is not required, . . . probable cause is not invariably required either. A search unsupported by probable cause can be constitutional, we have said, "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."

Id. (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987)).

in the particular context."[158] The Court considers three factors: (1) "the nature of the privacy interest upon which the search . . . at issue intrudes;"[159] (2) "the character of the intrusion;"[160] and (3) "the nature and immediacy of the government's concern . . . and the efficacy of [the search] for meeting it."[161] Cases where courts use this alternative reasonableness formula often involve civil authorities and usually do not involve criminal penalties.[162]

A closely related concept is the "community caretaking" doctrine, based on the notion that police serve to ensure the safety and welfare of the citizenry at large. Certain emergencies require an immediate government response,[163] known as a community caretaking function.[164] When an officer is pursuing a community caretaking function not involving seizure of a person, no particularized and objective justification is required.[165] Traditional constitutional requirements—warrant,

158. Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665-66 (1989).

159. *Vernonia*, 515 U.S. at 654.

160. *Id.* at 658.

161. *Id.* at 660.

162. *See, e.g., Vernonia*, 515 U.S. at 658 (observing "special needs" student-athlete drug test results were not turned over to law enforcement authorities or used for disciplinary action); *Von Raab*, 489 U.S. at 663 (noting "special needs" search results were not permitted to be given over to the government for prosecution); Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 621 (1989) (noting "special needs" administrative drug test results not sought for criminal prosecution, but rather from adherence to safety regulations). *See generally* Jennifer Y. Buffaloe, Note, *"Special Needs" and the Fourth Amendment: An Exception Poised to Swallow the Warrant Preference Rule*, 32 HARV. C.R.-C.L. L. REV. 529 (1997); Michael Polloway, Comment, *Does the Fourth Amendment Prohibit Suspicionless Searches—or do Individual Rights Succumb to the Government's "So-Called" Special Needs?*, 10 SETON HALL CONST. L.J. 143 (1999). The Supreme Court's most recent pronouncement on the "special needs" doctrine also suggests that the Fourth Amendment standard for biological testing turns, in great part, on whether the information will be used for law enforcement purposes, in which case, the Fourth Amendment standard is rigorous. Ferguson v. Charleston, No. 99-936, — U.S. —, 2001 WL 273220 (Mar. 21, 2001). By implication, where the information is not used for law enforcement purposes, the latitude offered to the government is broader.

163. *See* Camara v. Mun. Court of San Francisco, 387 U.S. 523, 539 (1967) (noting warrantless inspections have been "traditionally upheld in emergency situations"). The Court cited *North American Cold Storage Co. v. Chicago*, 211 U.S. 306 (1908) (seizure of unwholesome food), *Jacobson v. Massachusetts*, 197 U.S. 11 (1905) (compulsory smallpox vaccination), and *Kroplin v. Truax*, 165 N.E. 498 (Ohio 1929) (summary destruction of tubercular cattle). *See Camara*, 387 U.S. at 539.

164. *See* John F. Decker, *Emergency Circumstances, Police Responses, and Fourth Amendment Restrictions*, 89 J. CRIM. L. & CRIMINOLOGY 433, 451 (1999) (discussing *Camara*, 387 U.S. 523 (1967)).

165. *See* Cady v. Dombrowski, 413 U.S. 433, 441 (1973) (concluding community caretaker functions were not within the purview of normal warrant requirements because they are totally divorced from the detection, investigation, or acquisition

probable cause, etc.—do not apply to this form of police-citizen encounter. Government responses to such emergencies need not be judged by normal Fourth Amendment standards because they are not considered searches or seizures within the meaning of the Fourth Amendment.[166]

Courts use a three-prong test to determine whether police actions are justified as caretaking functions: (1) "there must exist an objectively reasonable basis for a belief in an immediate need for police assistance for the protection of life or substantial property interests;"[167] (2) the officer's actions "must be motivated by an intent to aid,"[168] rather than to solve a crime; and (3) "police action must fall within the scope of the emergency."[169]

Accordingly, four principles guide the remainder of this discussion. First, the breadth of discretion afforded to law enforcement authorities should be proportional to the magnitude and proximity of the risk. The more precise the definition of authority for law enforcement officials, and the more that rules of engagement distinguish real security concerns from police caprice, the broader the constitutionally permissible law enforcement authority. Second, counter-terrorism measures must not target persons or groups on the basis of their race or ethnicity or without probable cause. Third, law enforcement measures should be no more intrusive nor entail greater use of force than necessary under specific conditions. Measures likely to raise profound Fourth Amendment concerns, such as intrusion into private dwellings without probable cause, must be justified by an emergency that is both of great magnitude (i.e., the potential level of harm is great) and of great urgency (i.e., the necessity for immediate action outweighs the privacy interest). Measures justified by the necessity of a biological terrorism event may not be used as

---

of evidence relating to the violation of a criminal statute); *see also* Colorado v. Bertine, 479 U.S. 367, 381 (1987) (Marshall, J., dissenting) ("Inventory searches are not subject to the warrant requirement because they are conducted by the government as part of a community caretaking function").

166. *See Cady*, 413 U.S. at 441. *See generally* Mary Elisabeth Naumann, *The Community Caretaker Doctrine: Yet Another Fourth Amendment Exception*, 26 AM J. CRIM. L. 325 (1999); Philip B. Heymann, *The New Policing*, 28 FORDHAM URB. L.J. 407 (2000).

167. Decker, *supra* note 164, at 457.

168. *Id.* at 510.

169. *Id.* at 517.

a pretext to gain unwarranted access for searches nor to conduct other law enforcement activity. Finally, any legal action taken against any individual in connection with counter-terrorism must measure up to the requirements of the Fifth[170] and Sixth Amendments.[171]

b. Relevant Inquiries

Where public health and security are at stake, the legal issue is whether searches directly promote a government interest that outweighs the individual's interest in avoiding the intrusion.[172] This issue comprises six subsidiary questions.

First, how weighty or important is the government's interest? Searches may profoundly contribute to a government interest, but that government interest may be relatively insignificant. The more significant the government interest, the greater the scope given to the authority to conduct searches.

Second, how proximate is the relationship between the search and the government interest? If the search is only tangentially related to the interest, or if there are alternative ways of pursuing the interest, then the need for the search is manifestly reduced.

Third, how are persons or sites selected for searches, and does this selection methodology afford due process? An element of this inquiry is whether the method of selection

---

170. U.S. CONST. amend. V.

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Id.

171. U.S. CONST. amend. VI.

> In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.

Id.

172. *See generally* David S. Faigaman, *Reconciling Individual Rights and Government Interests: Madisonian Principles Versus Supreme Court Practice*, 78 VA. L. REV. 1521 (1992).

insinuates wrongdoing that might inappropriately diminish the individual's reputation. If the searches are entirely random and apply to virtually everyone within a given sector (e.g., random vehicle checkpoints), the search scheme may be more tolerable. On the other hand, if individuals are selected due to their racial or ethnic groupings, or if a few individuals are targeted for especially demeaning activity, that program of searches is more subject to challenge.[173]

Fourth, where is the search carried out? A search of a vehicle or of an individual in a public place is far more tolerable than searches of homes because of the high expectation of privacy an individual has when in his home.[174]

Fifth, how intrusive is the search—how much force is used, and what is the scope of the search? Protective sweep searches, conducted without a warrant but only superficially and only to determine whether a more intrusive search can be undertaken safely, are more tolerable than extensive searches backed by force.[175] At the opposite extreme, strip searches or body cavity searches are the least tolerable.

Finally, what use is made of evidence obtained in the search? Fewer legal concerns apply to searches to effectuate a government interest that is health-related and non-punitive. Also, a search from which only evidence is used which directly relates to the asserted prosecutorial purpose may be more tolerable than a search for a purpose that is a mere pretext for a wide-ranging prosecutorial investigation. Thus, Fourth Amendment problems are diminished if the law enforcement personnel overlook evidence of wrongdoing that is unrelated

173. *See* Whren v. United States, 517 U.S. 806, 813 (1996) (stating that the Constitution prohibits selective enforcement of the law based on considerations such as race); Brown v. City of Oneonta, 195 F.3d 111, 118-19 (2d Cir. 1999) (stating that an equal protection violation may be premised on police practice of conducting investigations utilizing racially based classifications); United States v. Avery, 137 F.3d 343, 354 (6th Cir. 1997) (holding that race cannot be the sole basis for conducting a search); *see also* Sheri L. Johnson, *Race and the Decision to Detain a Suspect*, 93 YALE L.J. 214 (1983).

174. *Compare* Cardell v. Lewis, 417 U.S. 583, 591 (1974) (holding warrantless search of motor vehicles permissible), *and* Terry v. Ohio, 392 U.S. 1 (1968) (holding warrantless search of person in public permissible given certain conditions), *with* Payton v. New York, 445 U.S. 573, 592 (1980) (prohibiting police from making warrantless and nonconsensual entry into suspects' homes in order to make routine felony arrests).

175. *See* Maryland v. Buie, 494 U.S. 325 (1990) (upholding the constitutionality of warrantless post-arrest protective sweep searches within a limited area).

to the asserted purpose of the search.

3. *Legal Treatment of Searches and Related Measures*

a. *Cordoning Areas, Preventing Ingress or Egress*

Courts have long held that officials may cordon off an area, establish a quarantine, or erect checkpoints for persons and/or vehicles leaving an area.[176] Both the need to prevent escape of suspected criminals[177] (or carriers of contagion[178]) and the individual's diminished right of privacy (on foot or in a vehicle) support this conclusion. Thus, there is no need to establish "emergency powers" to enable officials to cordon off areas.

b. *Compulsory Vaccinations and Other Medical Treatment*

Courts are likely to uphold compulsory medical interventions based upon a reasonable assessment of future harm. The courts have held that compulsory vaccinations during periods of contagious outbreaks do not violate due process.[179] Local, state, and federal government, therefore, may

176. *See* United States v. Martinez-Fuerte, 428 U.S. 543, 566 (1976) (holding stops for brief questioning at checkpoints are consistent with the Fourth Amendment and need not be authorized by a warrant); Jacobson v. Massachusetts, 197 U.S. 11, 25 (1905) (observing quarantine laws are authorized within the police power of the state to provide for public health and safety). The Supreme Court addressed the outer limits of the police power to use checkpoints this Term in *City of Indianapolis v. Edmond*, 121 S. Ct. 447 (2000) (holding that the city's drug interdiction checkpoints were in violation of the Fourth Amendment).

177. *See* Laaman v. U.S., 973 F.2d 107 (2d Cir. 1992) (involving alleged terrorist conspiracy to bomb military offices).

178. *See* Compagnie Française de Navigation à Vapeur v. La. State Bd. of Health, 186 U.S. 380 (1902) (preventing immigrants from a potentially infected area from entering the country).

179. *See, e.g.*, Jacobson, 197 U.S. at 26.

> [T]he liberty secured by the Constitution of the United States to every person within its jurisdiction does not import an absolute right in each person to be, at all times and in all circumstances, wholly freed from restraint. There are manifold restraints to which every person is necessarily subject for the common good.... [A] community has the right to protect itself against an epidemic of disease which threatens the safety of its members. It is to be observed that when the regulation in question was adopted smallpox, according to the recitals in the regulation adopted by the board of health, was prevalent to some extent in the city of Cambridge, and the disease was increasing. If such was the situation,—and nothing is asserted or appears in the record to the contrary, —if we are to attach, any value whatever to the knowledge which, it is safe to affirm, in common to all civilized peoples touching smallpox and the

legally vaccinate those deemed at risk. A more difficult legal question is presented by quarantines of contagious patients. There have been cases of communicable diseases where courts have required persons to be actually infectious to be subject to isolation or quarantine.[180] These cases, however, are distinguishable because the individual was completely deprived of liberty based on scarce evidence of a current or imminent danger to public health. In cases where the state could demonstrate a "rational nexus" between a relatively non-intrusive intervention and the likely reduction in future harm to the public, there has been little judicial inclination to interfere with reasonable medical judgments.

Court precedents from HIV cases, however, weigh heavily in favor of protecting due process rights, thereby strengthening the "rational nexus" requirement. In *Hill v. Evans*,[181] an Alabama statute was held to violate equal protection because it allowed uninformed, non-consensual HIV testing of persons who seek medical services on the basis of a physician's judgment that the person is at high risk for HIV.[182] The court found the absence of a consent requirement unconstitutional because the State "did not establish that the ability of physicians to test without informed consent individuals they consider to be high risk for the HIV virus, for that reason alone, would in any way curb the spread of the disease."[183] The court, however, upheld a medical care exception allowing non-consensual HIV testing where medical treatment might be modified due to the presence or absence of HIV. The court found that "there is a legitimate government interest in a treating physician knowing the HIV status of a patient . . . [and] that governmental interest outweighs the . . . privacy interest of

---

methods most usually employed to eradicate that disease, it cannot be adjudged that the present regulation of the board of health was not necessary in order to protect the public health and secure the public safety.

Id. at 26-28.

180. *See, e.g., In re* Halko, 54 Cal. Rptr. 661, 664-65 (1966) (requiring reasonable grounds to believe the person is actually infected (and contagious) in order to justify restraint of personal liberty); People *ex. rel.* Barmore v. Robertson, 134 N.E. 815, 819 (1922) (stating that a person cannot be quarantined upon mere suspicion that he may have a contagious and infectious disease).

181. No. 91-A-626-N, 1993 WL 595676 (M.D. Ala. Oct. 7, 1993).

182. *See id.* at *4-*6.

183. *Id.* at *7.

an individual."[184]

Thus, two issues emerge. First, how are individuals selected for testing or treatment? Second, does the justification for the particular testing or treatment justify the intrusion into the individual's privacy? Legislation can effectively address each of these issues, as discussed below.[185]

c. Lowering the Threshold of Reasonable Suspicion

The suggestion of authorizing searches in the absence of normally sufficient evidence misconstrues the critical issues discussed above. If the search is directed specifically at someone thought to be a terrorist, the typical "reasonable suspicion" standard is appropriate. In view of the low threshold of this standard, officials will not be unreasonably limited in the actions they can undertake. If the search is directed more broadly than at a designated suspect, no lowering of the threshold of reasonable suspicion is relevant. For example, in the apartment hypothetical discussed earlier, there is no reasonable suspicion whatsoever as to the innocent dwellers in five of the six apartments, and no lower threshold could justify individual searches of their dwellings. This problem is the Fourth Amendment rendition of Russian roulette. Only enabling sweep searches, as discussed below, can address this issue.

d. Sweep Searches

Intrusive sweep searches into dwellings have been judicially struck down on a number of occasions, but in each case the State failed to establish the necessity of those searches.[186] Most notably, the Chicago Housing Authority (CHA) attempted to control the rising instances of violence and drug crimes in its public housing by staging a surprise assault on its public housing projects: all entrances and exits were sealed, and every apartment was searched for drugs, weapons, and illegal

---

184. *Id.* at *12.

185. *See infra* Part III.D.4.

186. *See, e.g.*, Steagald v. United States, 451 U.S. 204 (1981) (holding officers' search unconstitutional without requisite consent of exigent circumstances); Pratt v. Chicago Hous. Auth., 848 F. Supp. 792 (N.D. Ill. 1994) (holding searches conducted in the absence of probable cause or exigent circumstances unconstitutional).

residents.[187] The CHA claimed that the searches were justified by the emergency circumstances of high crime and drug use and were necessary to protect the safety and welfare of tenants. Although the dispute was never litigated to a conclusion, most commentators agree that the CHA confused the meaning of the term "emergency" by substituting a *serious* concern with crime for criteria that focus on the necessity of *urgent* action.[188]

Intrusion into private dwellings without probable cause to believe that there is evidence of a crime inside raises the most profound Fourth Amendment considerations and must, therefore, be justified by an emergency that is both of great magnitude (i.e., the potential level of harm is great) and of great urgency (i.e., the necessity for immediate action outweighs the privacy interest). No case law has been found where this test has been satisfied, but neither has case law been found which has struck down official action in response to mass disaster or contagion.

4. *Can Anything Be Done To Clarify or Expand Emergency Powers?*

Neither Congress nor the Executive Branch can promulgate laws that would contravene or diminish the operative scope of the Fourth Amendment.[189] Manifestly unconstitutional behavior cannot be made legal because Congress so legislates. Yet Congress can address the questions outlined above and, in so doing, both overtly define the need asserted to justify the searches and corral law enforcement to ensure that appropriate boundaries are respected. Accordingly, Congress can take at least six possible steps.

First, Congress can explicitly articulate the government interest at stake in bioterrorism cases and expound on the magnitude of that interest. Legislation to address biological

187. *See Pratt*, 848 F. Supp. at 792.

188. *See* Andrew Byers, Note, *The Special Government Needs Exception: Does It Allow for Warrantless Searches of Public Housing?*, 41 WAYNE L. REV. 1469 (1995); Zionne N. Presley, Note, *Privacy or Safety: A Constitutional Analysis of Public Housing Sweep Searches*, 6 B.U. PUB. INT. L.J. 777 (1977); Monica L. Selter, Comment, *Sweeps: An Unwarranted Solution to the Search for Safety in Public Housing*, 44 AM. U. L. REV. 1903 (1995).

189. *See* District of Columbia v. Little, 178 F.2d 13, 19 (D.C. Cir. 1949), *aff'd*, 339 U.S. 1 (1950); *cf.* Dickerson v. United States, 120 S. Ct. 2326, 2329 (2000) (ruling that Congress may not legislatively supersede a "constitutional decision" of the United States Supreme Court).

terrorism obviously can identify the enormous interests to the public and to national security that compel extraordinary preventive and responsive measures. Indeed, the certainty of this identification probably renders congressional action unnecessary.

Second, Congress can specify that a threat of biological terrorism is an "emergency" and can mandate that the President so designate. This designation would satisfy the legal requirement that broader-than-normal law enforcement powers be exercised only during periods of emergency. Moreover, Congress can specify that enumerated measures be undertaken to address this type of emergency.

Third, Congress can authorize and specify the implementation of appropriate medical measures to prevent harm, including vaccination and quarantine programs.

Fourth, Congress can express its view on the relevance of searches to protecting or promoting the articulated government interests. More specifically, Congress can address the difficulty that standard law-enforcement methods might face in detecting easily concealable but highly dangerous items. In connection with presidential identification of explicitly specified cases of biological terrorism, specific powers to conduct limited and necessary sweep searches may be granted.

Fifth, Congress can specify the selectivity, location, and intrusiveness of searches and identify how the characteristics of the search scheme correspond to the interest to be promoted. These specifications would be analogous to those for warrantless searches of commercial sites conducted pursuant to an administrative search scheme.[190] By specifying the regulatory interest and by tailoring the search scheme to that interest, Congress can go far toward establishing that a particular search, if conducted within the scope of that scheme, is reasonable under the Fourth Amendment.[191]

Finally, Congress can implement means to ensure that searches permitted by the necessity of a biological terrorism event may not be used as a subterfuge to gain access to sites

190. *See* Edward A. Tanzman & Barry Kellman, *Legal Implementation of the Multilateral Chemical Weapons Convention: Integrating International Security with the Constitution*, 22 N.Y.U. J. INT'L L. & POL. 475, 506-08 (1990).

191. *See id.* at 508-09.

without a warrant and search for an array of criminal activity.

CONCLUSION

The unique, low probability, high-magnitude risk of bioterrorism confounds the formulation of legal responses. Legal responses, however, are at best a part of the policy picture; other disciplines must contribute their own responses if a coherent and comprehensive strategy is to be implemented. In an even larger sense, the measures that are formulated to respond to the threat of bioterrorism should be part of broader international efforts to control and eliminate weapons of mass destruction. In every conceivable dimension, uncertainty reigns.

Yet this much is certain: with regard to biological terrorism, there is capability and there is motivation. The threat of biological weapons is spreading as technological hurdles diminish and more people in more nations develop the capabilities to produce and use such weapons. The United States cannot ignore the manifestations—both at home and abroad—of the extraordinary hate which motivates such terrorism. If a bioterrorist attack happens, we will all be victims. If we do not do what we can to prevent it, we will all be culprits.