THE FUTURE OF THE CONSTITUTION

December 08, 2010

Reuters/Jim Young

Innovation's Darker Future: Biosecurity, Technologies of Mass Empowerment, and the Constitution

Benjamin Wittes

Governance Studies at BROOKINGS

INTRODUCTION

Using gene-splicing equipment available online and other common laboratory equipment and materials, a molecular biology graduate student undertakes a secret project to recreate the smallpox virus. Not content merely to bring back an extinct virus to which the general population is now largely naïve, he uses public source material to enhance the virus's lethality, enabling it to infect even those whom the government rushes to immunize. His activities raise no eyebrows at his university lab, where synthesizing and modifying complex genomes is even more commonplace and mundane by 2025 than it is today. While time-consuming, the task is not especially difficult. And when he finishes, he infects himself and, just as symptoms begin to emerge, he proceeds to have close contact with as many people from as many possible walks of life as he can in a short time. He then kills himself before becoming ill and is buried by his grieving family with neither they nor the authorities having any idea of his infection.

Benjamin Wittes is a senior fellow and research director in Public Law at the Brookings Institution. He is also a co-founder of the *Lawfare* blog and has written extensively on the relationship between law and security.

The outbreak begins just shy of two weeks later and seems to come from everywhere at once. Because of the virus's long incubation period, it has spread far by the time the disease first manifests itself. Initial efforts to immunize swaths of the population prove of limited utility because of the perpetrator's manipulations of the viral genome. Even efforts to identify the perpetrator require many months of forensic effort. In the meantime, authorities have no idea whether the country—and quickly the world—has just suffered an attack by a rogue state, a terrorist group, or a lone individual. Dozens of groups around the world claim responsibility for the attack, several of them plausibly.

The government responds on many levels: It moves aggressively to quarantine those infected with the virus, detaining large numbers of people in the process. It launches a major surveillance effort against the enormous number of people with access to gene synthesis equipment and the capacity to modify viral genomes in an effort to identify future threats from within American and foreign labs. It attempts to restrict access to information and publications about the synthesis and manipulation of pathogenic organisms—suddenly classifying large amounts of previously public literature and blocking publication of journal articles that it regards as high-risk. It requires that gene synthesis equipment electronically monitor its own use, report on attempts to construct sequences of concern to the government, and create an audit trail of all synthesis activity. And it asks scientists all over the world to report on one another when they see behaviors that raise concerns. Each of these steps produces significant controversy and each, in different ways, faces legal challenge.

The future of innovation has a dark and dangerous side, one we dislike talking about and often prefer to pretend does not, in fact, loom before us. Yet it is a side that the Constitution seems preponderantly likely to have to confront—in 2025, at some point later, or tomorrow. There is nothing especially implausible about the scenario I have just outlined—even based on today's technology. By 2025, if not far sooner, we will likely have to confront the individual power to cause epidemics, and probably other things as well.

Technologies that put destructive power traditionally confined to states in the hands small groups and individuals have proliferated remarkably far. That proliferation is accelerating at an awe-inspiring clip across a number of technological platforms. Eventually, it's going to bite us hard. The response to, or perhaps the anticipation of, that bite will put considerable pressure on constitutional norms in any number of areas.

We tend to think of the future of innovation in terms of intellectual property issues and such regulatory policy questions as how aggressive antitrust enforcement ought to be and whether the government should require Internet neutrality or give carriers latitude to favor certain content over other content. Broadly speaking, these questions translate into disputes over which government policies best foster innovation—with innovation presumed to be salutary and the government, by and large, in the position of arbiter between competing market players.

But confining the discussion of the future of innovation to the relationship among innovators ignores the relationship between innovators and government itself. And government has unique equities in the process of innovation, both because it is a huge consumer of products in general and also because it has unique responsibilities in society at large. Chief among these is security. Quite apart from the question of who owns the rights to certain innovations, government has a stake in who is developing what—at least to the extent that some innovations carry significant capacity for misuse, crime, death, and mayhem.

This problem is not new—at least not conceptually. The character of the mad scientist muh-huh-huhing to himself as he swirls a flask and promises, "Then I shall destroy the world!" is the stuff of old movies and cartoons. In literature, versions of it date back at least to Mary Shelley in the early 19th century. Along with literary works set in technologically sophisticated dystopias, it is one of the ways in which our society represents fears of rapidly evolving technology.

The trouble is that it is no longer the stuff of science fiction alone. The past few decades have seen an ever-augmenting ability of relatively small, non-state groups to wage asymmetric conflicts against even powerful states. The groups in question have been growing smaller, more diffuse, and more loosely knit, and technology is both facilitating that development and dramatically increasing these groups' ultimate lethality. This trend is not futuristic. It is already well under way across a number of technological platforms—most prominently the life sciences and computer technology. For reasons I shall explain, the trend seems likely to

continue, probably even to accelerate. The technologies in question, unlike the technologies associated with nuclear warfare, were not developed in a classified setting but in the public domain. They are getting cheaper and proliferating ever more widely for the most noble and innocent of reasons: the desire to cure disease and increase human connectivity, efficiency, and capability. As a global community, we are becoming ever more dependent upon these technologies for health, agriculture, communications, jobs, economic growth and development, even culture. Yet these same technologies—and these same dependencies—make us enormously vulnerable to bad actors with access to them. Whereas once only states could contemplate killing huge numbers of civilians with a devastating drug-resistant illness or taking down another country's power grids, now every responsible government must contemplate the possibility of ever smaller groupings of people undertaking what are traditionally understood as acts of war. We have already seen the migration of the destructive power of states to global non-state actors, particularly Al Qaeda. We can reasonably expect that migration to progress still further. It ultimately threatens to give every individual with a modest education and a certain level of technical proficiency the power to bring about catastrophic damage. Whereas governments once had to contemplate as strategic threats only one another and a select bunch of secessionist militias and could engage with individuals as citizens or subjects, this trend ominously promises to force governments to regard individuals as potential strategic threats. Think of a world composed of billions of people walking around with nuclear weapons in their pockets.[1]

If that sounds hyperbolic, it is probably only a little bit hyperbolic. As I shall explain, the current threat landscapes in the life sciences—the area which I use in this paper as a kind of case study—is truly terrifying. (No less so is the cyber arena, an area Jack Goldsmith is treating in detail and where attacks are already commonplace.) The landscape is likely to grow only scarier as the costs of gene synthesis and genetic engineering technologies more generally continue to plummet, as their capacity continues to grow, and as the number of people capable individually or in small groups of deploying them catastrophically continues to expand. The more one studies the literature on biothreats, in fact, the more puzzling it becomes that a catastrophic attack has not yet happened.

Yet biothreats alone are not the problem; the full problem is the broader category of threats they represent. Over the coming decades, we are likely to see other areas of technological development that put enormous power in the hands of individuals. The issue will not simply be managing the threat of biological terrorism or biosecurity more broadly. It will be defining a relationship between the state and individuals with respect to the use and development of such dramatically empowering new technologies that both permits the state to protect security and at once insists that it does so without becoming oppressive.

[1] See Remarks by Professor James Fearon, Remarks at Columbia University's Symposium on Constitutions, Democracy, and the Rule of Law: Catastrophic Terrorism and Civil Liberties in the Short and Long Run (Oct. 17, 2003), (transcript available at http://www.stanford.edu/~jfearon/papers/civlibs.doc).

To state this problem is to raise constitutional questions, and I'm not entirely sure that a solution to it exists. Governments simply cannot regard billions of people around the world as potential strategic threats without that fact's changing elementally the nature of the way states and those individuals interact. If I am right that the biotech revolution potentially allows individuals to stock their own WMD arsenals and that other emergent technologies will create similar opportunities, government will eventually respond—and dramatically. It will have no choice.

But exactly how to respond—either in reaction or in anticipation—is far from clear. Both the knowledge and the technologies themselves have proliferated so widely to begin with that the cat really is out of the bag. Even the most repressive measures won't suffice to stuff it back in. Indeed, the options seem rather limited and all quite bad: intrusive, oppressive, and unlikely to do much good.

And it is precisely this combination of a relatively low probability of policy success, high costs to other interests, and constitutional difficulties that will produce, I suspect, perhaps the most profound change to the Constitution emanating from this class of technologies. This change will not, ironically, be to the Bill of Rights but to the Constitution's most basic assumptions with respect to security. That is, the continued proliferation of these technologies will almost certainly precipitate a significant erosion of the federal government's monopoly over security policy. It will tend to distribute responsibility for security to thousands of private sector and university actors whom the technology empowers every bit as much as it does would-be terrorists and criminals. This point is perhaps clearest in the context of cybersecurity, but it is also true in the biotech arena, where the best defense against biohazards, man-made and naturally occurring alike, is good public health infrastructure and more of the same basic research that makes biological attacks possible. Most of this research is going on in private companies and universities, not in government; the biotech industry is not composed of a bunch of defense contractors who are used to being private sector arms of the state. Increasingly, security will thus take on elements of the distributed application, a term the technology world uses to refer to programs which rely on large numbers of networked computers all working together to perform tasks to which no one system could or would devote adequate resources. While state power certainly will have a role here—and probably an uncomfortable role involving a lot of intrusive surveillance—it may not be the role that government has played in security in the past.

The Biosecurity Problem

The American constitutional system has had to respond before to the development of technologies that threaten to enhance the destructive power of dangerous people, and its response has varied significantly. The First Congress regarded firearms as sufficiently valuable as a means of defending states against federal power that it affirmatively protected "the right of the People to Keep and Bear Arms"—notwithstanding the fact that guns also facilitated robbery, dueling, and

murder. Faced with a potentially dangerous technology, the Founders created a constitutional right to use it. By contrast, the government tightly controlled the development of nuclear technology—restricting access both to nuclear materials and to information about how to use those materials to manufacture weapons. It directly sponsored and controlled nuclear weapons research from the beginning. (For many years, it took a similar approach to much cryptography, and to some extent it still does.) The judgment with respect to nuclear technologies was that nuclear weapons were so dangerous that the state's monopoly on their creation and stockpiling—not to mention their use—should be total.

The class of technologies with which I am concerned here—of which biotechnology is a paradigmatic example—have certain characteristics both in common with and dissimilar to both firearms and nuclear technologies. These characteristics make them difficult to place along the spectrum those innovations describe.

First, unlike nuclear technologies, the biotechnology revolution did not develop principally in classified settings at government-run labs, with the government controlling access to the key materials. It involves at this stage widely disseminated technologies that depend on readily available training and materials. It developed in public in open dialogue with non-military purposes in mind, and its overwhelming uses—even by governments—remain non-military. We didn't sequence the human genome in order to figure out how to design viruses to kill people. Yet among the many salutary results of biotechnology—everything from better medicines, more productive agriculture, and promising new approaches to energy and environmental stewardship—are some not-so-salutary consequences. To wit, a public literature now exists that teaches bad guys how to do horrific things—and the materials, unlike highly enriched uranium, are neither scarce nor expensive.

Second, the destructive technologies are, at least to some degree, hard to separate from the socially beneficial technologies that give rise to them. The research on how to use genetics to cure and prevent disease *can often also be used to cause disease*. Defensive research can potentially empower the bad guys, as well as the good guys—at least if it gets published. Yet since everyone seems to agree that, in the long run, good public health policy in general represents a big part of the answer to biosecurity threats—whether naturally occurring ones, accidents, or intentional man-made disasters—and since public health policy is far broader than bioterrorism prevention, policies that impair basic research will almost certainly be both counterproductive and ineffective.

Third, the misuse of these technologies blurs the distinction between foreign and domestic threats and, indeed, makes attribution of any attack extremely difficult. As every student in a biological laboratory (not to mention every individual on his home computer) becomes a possible threat to national security, traditional techniques of surveillance, deterrence, and non-proliferation become increasingly ill-suited to detecting and preventing terrorist activity. In the case of

the 2001 anthrax attacks, for example, attribution took seven years and remains to this day contested. Indeed, often in these cases, a target state will not be able to determine whether its attacker is another state, a political group, a criminal group, or a lone wolf.

Indeed, the life sciences now threaten realistically to put the power of a WMD attack in the hands if not of the average person, certainly of many above-average people with relatively inexpensive equipment and basic training in genetic engineering. Biological weapons are unique among weapons of mass destruction in that they have the capacity, like nuclear weapons, to produce truly catastrophic damage, yet, like chemical weapons, are comparatively inexpensive and easy to produce. The technology required for their production is generally the same as the technology used in legitimate life-sciences research; indeed, it is the bread-and-butter stuff of the biotech revolution that has done so much good throughout the world. Precisely because modern biotechnology has so much promise and offers so many benefits in so many walks of life, the materials and skills required to develop these weapons are not rare. So while it may be difficult for even a highly trained individual to build his own nuclear weapon, an individual with relatively modest expertise and resources could potentially obtain or develop his own biological weapon with worldwide consequences. As costs continue to fall, the number of people around the world whom governments will have to regard—at least in theory—as capable of having their own personal WMD program grows commensurately.

This is already happening fast. Princeton bioterrorism expert Christopher Chyba has likened the proliferation of gene synthesis capability to the explosion in computer technology known as Moore's Law. Intel Corp.'s co-founder Gordon Moore observed decades ago that the number of transistors on an integrated circuit was doubling every two years—a trend that has remained true ever since. Chyba writes that "[j]ust as Moore's law led to a transition in computing from extremely expensive industrial-scale machines to laptops, iPods, and microprocessors in toys, cars, and home appliances, so is biotechnological innovation moving us to a world where manipulations or synthesis of DNA will be increasingly available to small groups of the technically competent or even individual users, should they choose to make us of it."[2] Chyba notes that the cost of synthesizing a human genome is nose-diving,[3] and along with cost decreases, the efficiency of biotechnology continues to increase. While it took researchers at the State University of New York three years to synthesize the complete polio virus in 2002, the following year, a different group of researchers synthesized a viral genome of comparative length in only two weeks.[4]

Furthermore, biological weapons do not work like other weapons of mass

[2] C.F. Chyba, "Biotechnology and the Challenge to Arms Control," *Arms Control Today* 30, no. 8 (October 2008): 12.
[3] Ali Nouri and C.F. Chyba, "Proliferation-Resistant Biotechnology: An Approach to Improve Biosecurity," *Nature Biotechnology* 27, no. 3 (March 2009): 234.
[4] Chyba, "Biotechnology and the Challenge to Arms Control," 12.

destruction. The long incubation periods for many pathogens mean that an infected individual can travel and infect others before contamination becomes apparent, making it difficult to limit the impact of an attack. Moreover, illnesses caused by biological weapons are often hard to distinguish from naturally occurring outbreaks. It took investigators a year to realize that an outbreak in 1984 of salmonella in Oregon was the result of an attack by followers of the Bagwan Shree Rajneesh cult, for example.[5] The difficulty of attribution, combined with the fact that authorities may not learn of an attack until symptoms emerge days or weeks after infection, blunts the effectiveness of traditional models of deterrence and response.

What's more, deadly pathogens are not that hard to come by. Many occur naturally; notable naturally occurring pathogens include anthrax, bubonic plague, hemorrhagic fevers such as Ebola and Marburg, Tularemia, and Venezuelan Equine Encephalitis. These can be collected in the natural environment, a fact that was not lost on the notorious Japanese cult Aum Shinrikyo—which attempted to obtain Ebola strains in Zaire. In addition, many pathogens are stockpiled by commercial entities for entirely legitimate purposes, although controls on these stockpiles have tightened in recent years.

And as our introductory nightmare scenario makes clear, even pathogens like smallpox and the 1918 flu virus, which have been wiped out in the wild, can now be recreated. The literature *available in the public domain* describing—even routinizing—genetic engineering projects involving the creation and enhancement of deadly pathogens should be at least as terrifying to policymakers around the world as box cutters or guns on airplanes. Viral genomes are relatively small. Many have already been mapped, and the materials required to modify existing sequences to mirror them or to synthesize them from scratch are all commercially available. And scientists have repeatedly demonstrated that if terrorists—or individual bad guys—have the will, science has a way:

- In 2001, Australian researchers published the results of a study in which they used gene splicing technology to create a variation of the mousepox virus both more lethal to mice than the normal one and impervious to vaccination.[6] (Mousepox is a virus closely related to human smallpox but which does not cause disease in humans.)
- In 2001, a team of virologists in Germany and France constructed the Ebola virus from three strands of complementary DNA.[7]
- In 2002, researchers from the State University of New York, Stony Brook, published studies of de novo DNA synthesis of the polio virus,

[5] C.F. Chyba, "Toward Biosecurity," *Foreign Affairs* 81, no. 3 (May/June 2002): 129.
[6] R.J. Jackson et al., "Expression of a Mouse Interleukin-4 by a Recombinant Ectromelia Virus Represses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox," *Journal of Virology* 45, no. 3 (February 2001): 1205-10.
[7] V.E. Volchkov et al., "Recovery of Infectious Ebola Virus from Complementary DNA: RNA editing of the GP gene and viral cytotoxicity," *Science* 291 (March 2001): 1965-69.

which they had constructed using nucleotide fragments purchased from a mail-order biotech company.[8]

- In similar studies, scientists have successfully synthesized the 1918 Spanish influenza virus,[9] which infected an estimated one-third of the world's population and killed between 50 and 100 million people worldwide,[10] and Encephalomyocarditis virus, which can cause fatal febrile illness in humans.[11]

To be sure, technological obstacles still remain to terrorist groups or individuals in launching a global pandemic, but these obstacles are growing ever more surmountable. As technology continues to improve, the creation of larger, more complex pathogens—including, potentially, the smallpox virus[12]—will become cheaper and easier for a wider array of potential bad actors.

And if recent history is any guide, that's an ominous possibility. For although no state, terrorist group, or individual has yet successfully launched a mass-casualty biological attack, a range of cases demonstrate that there is no dearth of people who would like to do so. Aum Shinrikyo expended great effort in the early 1990s attempting to obtain biological weapons. Before killing twelve people and injuring more than 5,000 by releasing sarin nerve gas on a train in Tokyo, cult members attempted to release botulinum toxin in the Japanese Parliament, sent a mission to Zaire to obtain strains of the Ebola virus, and released anthrax spores from atop a building in Tokyo.[13] The case of Larry Wayne Harris provides another chilling example of a non-state actor's potential bioterrorism capabilities. Harris was a member of the Aryan Nations who easily obtained the bacterial agent of the bubonic plague from a private company using the stationery of a fictitious laboratory. After the company shipped the bacterial cultures to his home, an employee became concerned and contacted the Centers for Disease Control. Thus alerted, the authorities obtained a search warrant and discovered pathogens, as well as explosives, in Harris's car and at his home. Harris explained that he was stockpiling weapons in preparation for an imminent Armageddon.[14]

And, of course, the threat of bioterrorism became a reality with the anthrax attacks in October 2001. Just weeks after the attacks on September 11, 2001, someone mailed anthrax-contaminated powder from a mailbox in Princeton, N.J.,

---

[8] J. Cello, A. V. Paul, and E. Willmer, "Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template," *Science* 297 (August 9, 2002): 1016-18.
[9] T.M. Tumpey et al., "Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus," *Science* 310 (October 7, 2005): 77-80.
[10] Jeffery K. Taubenberger and David M. Morens, Center for Disease Control, "1918 Influenza: the Mother of All Pandemics," (January 2006), available at http://www.cdc.gov/ncidod/eid/vol12no01/05-0979.htm.
[11] Y.V. Svitkin and N. Sonenberg, "Cell-free Synthesis of Encephalomyocarditis Virus," *Journal of Virology* 77, no. 11 (2003): 6551-55.
[12] A. Rabodzey, "Biosecurity Implications of the Synthesis of Pathogenic Viruses," *Politics and Life Sciences* 22, no. 2 (2003): 44-49.
[13] Barry Kellman, "Biological Weapons: Legal Measures for Preventing Catastrophe," *Harvard Journal of Law and Public Policy* 24 (2001): 425.
[14] Ibid., 449-50.

killing five people, injuring 17, shutting down mail services and resulting in the evacuation of federal buildings, including Senate offices and the Supreme Court. Although the Justice Department closed its investigation in 2008 after the prime suspect, a bio-defense employee named Bruce E. Ivins, committed suicide, doubts still linger about the case.[15] In any event, the fact that it took seven years for investigators to develop an indictable case against a single individual illustrates the security and law enforcement challenges posed by even a relatively low-impact bioterrorism event.

If a terrorist were to overcome the challenges inherent in developing a naturally occurring pathogen into a deployable weapon, the consequences could be devastating. The U.S. Office of Technology Assessment has estimated, for example, that an airplane flying over a densely populated area such as Washington, D.C. could kill as many as three million people with 100 kilograms of properly aerosolized anthrax.[16] A contagious virus specifically engineered for lethality against a relatively unimmunized population could, at least theoretically, be worse. In the world of low-probability, high-impact events, this type of attack stands out for its relative plausibility.

Attempts at Governance to Date

It rather understates the matter to say that current governance of biosecurity is hopelessly inadequate to the task of preventing the disasters one might reasonably anticipate. This is not chiefly a function of the fact that changing governance in a fashion that carries real costs in the absence of some dramatic precipitating event is always difficult—though that fact plays a big role as well. It also reflects the fact that the ideal governance approach is far from obvious. Indeed, nobody quite knows how to approach the problem or even whether an effective governance structure exists. Even if one could, for example, classify all of the relevant now-public literature and slap strict controls on the technologies in question, who would want to? The biotechnology revolution is a wonderful thing, and it has depended pervasively on precisely the open culture which has created the vulnerabilities I have been describing. In any event, too many people have too deep an understanding of how genetic engineering works for the public to forget what it knows—and the Internet would ensure that we could not easily suppress dangerous papers if we tried.

The problem with current governance is not that we don't have laws

---

[15] See Scott Shane, "Critics of Anthrax Inquiry Seek an Independent Review," *The New York Times* (September 24, 2008), http://query.nytimes.com/gst/fullpage.html?res=9D03E4DB153DF937A1575AC0A96E9C8B63; Jobby Warrick, Marilyn W. Thompson, and Aaron C. Davis, "Scientist Question FBI Probe on Anthrax," *Washington Post* (August 3, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/08/02/AR2008080201632.html.

[16] Office of Technology Assessment, *Proliferation of Weapons of Mass Destruction: Assessing the Risk, OTA-ISC-559* (Washington, DC: U.S. Government Printing Office, August 1993), 53-54, http://www.au.af.mil/au/awc/awcgate/ota/9341.pdf.

prohibiting abuse of biotechnology. We do. The law, in fact, over the past decade has developed rather admirably, and nobody now could do anything horrible without running afoul of it. Nonetheless, current law isn't likely to do much more than inconvenience someone seriously committed to developing or releasing a biological agent that could do great damage. The law does not—and probably cannot—address the attribution problems at work here effectively, nor can it easily offer much in the way of prevention.

Traditionally, states have treated biothreats either as naturally occurring phenomena viewed through the lens of public health policy or as problems of state-to-state weapons proliferation. For example, the 1972 Biological and Toxin Weapons Convention ("BWC"), ratified by the United States in 1975, saw the problem of biological weapons almost entirely in terms of official biological state warfare programs—a function of the fact that, back then, it really was science fiction to imagine anyone but a state developing or using significant biological weapons.[17] The restrictions of the BWC in the United States did not even apply to private individuals until the passage of the Biological Weapons Anti-Terrorism Act of 1989, which criminalized the individual production, possession, and transfer of biological agents "for use as a weapon."[18]

Congress stepped into the fray again following the September 11 attacks and the fatal anthrax mailings shortly thereafter, passing two pieces of additional legislation. The PATRIOT Act strengthened the biological weapons statute to make it a crime to possess any "biological agent, toxin, or delivery system of a type or in a quantity that . . . is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose."[19] The PATRIOT Act also prohibited the possession of certain listed biological agents by a "restricted person"—or their transfer to such a person.[20]

Second, Congress passed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 to regulate the possession, transfer, and

---

[17] "Convention on the Development and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction," April 10, 1972, *Treaty Series: Treaties and International Agreements Registered or Filed or Recorded with the Secretariat of the United Nations*.

[18] *Biological Weapons Anti-Terrorism Act of 1989, U.S. Code* 18 (1990), § 175.

[19] *USA PATRIOT Act*, Public Law 107-56, 115 Stat. 272, Title VIII (October 26, 2001), § 817 (amending *Biological Weapons Act* § 175).

[20] Ibid. at 115 Stat. 386 (adding to *Biological Weapons Act* sections § 175b(a)(1) and (d)(2)). A "restricted person" was defined as a person who "(A) is under indictment for a crime punishable by imprisonment for a term exceeding 1 year; (B) has been convicted in any court of a crime punishable by imprisonment for a term exceeding 1 year; (C) is a fugitive from justice; (D) is an unlawful user of any controlled substance (as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802)); (E) is an alien illegally or unlawfully in the United States; (F) has been adjudicated as a mental defective or has been committed to any mental institution; (G) is an alien (other than an alien lawfully admitted for permanent residence) who is a national of a country as to which the Secretary of State, … has made a determination (that remains in effect) that such country has repeatedly provided support for acts of international terrorism; or (H) has been discharged from the Armed Services of the United States under dishonorable conditions." In 2004 Congress added "(I) is a member of, acts for or on behalf of, or operates subject to the direction or control of, a terrorist organization as defined in section 212(a)(3)(B)(vi) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)(vi))." *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law 108-458.

use of select biological agents. The new law required the Secretary of Health and Human Services to, "by regulation establish and maintain a list of each biological agent and each toxin that has the potential to pose a severe threat to public health and safety."[21] It also directed the Secretary to provide for the "establishment and enforcement of safety procedures for the transfer" of designated agents as well as for their "possession and use."[22] The regulations had to require "registration with the Secretary" as a prerequisite for possession, use, or transfer and had to "include provisions to ensure that persons seeking to register under such regulations have a lawful purpose to possess, use, or transfer such agents and toxins."[23] Registration required applicants to provide "information regarding the characterization of listed agents and toxins to facilitate their identification, including their source." Finally, the statute further required the Department to "maintain a national database that includes the names and locations of registered persons, the listed agents and toxins such persons are possessing, using, or transferring, and information regarding the characterization of such agents and toxins."[24] Implementing the congressional mandate, HHS regulations prohibited the regulated entities and individuals from transferring such agents to non-registered entities and individuals, and also authorized the Inspector General of the Department to investigate violations and impose civil penalties.[25] The 2002 act also created additional criminal liability for unauthorized shipping, transfer, and possession of select agents.[26]

One of the most important, and most controversial, of the Bioterrorism Response Act's sections provided for a rudimentary background check for people registering to handle select agents to make sure they were not excluded from doing so by the statute's enumerated categories.[27] This effectively authorized the Attorney General to require anyone seeking access to listed biological agents to submit to a "security risk assessment." The regulations implementing this provision permit the FBI to share an applicant's information with other governmental agencies, including law enforcement and private organizations.[28] Some in the scientific community have expressed concern that the security risk

---

[21] *Public Health Security and Bioterrorism Preparedness and Response Act of 2002,* Public Law 107-188, 116 Stat. 594, § 8401 et seq. Regulations would define as "select agents" the biological agents and toxins on this list. U.S. Code of Federal Regulations 42 § 73.1 (April 18, 2005) (defining "[s]elect agent and/or toxin").

[22] Ibid, Sec. 315A.

[23] Ibid.

[24] Ibid.

[25] U.S. Code of Federal Regulations 42 § 73.16 ("a select agent or toxin may only be transferred to individuals or entities registered to possess, use, or transfer that agent or toxin"); ibid. § 73.21 (defining civil penalties).

[26] *Public Health Security and Bioterrorism Preparedness and Response Act of 2002,* Sec. 231.

[27] Ibid., Sec. 351A(e)(3)(B). The statute essentially denies registration to any "restricted person," as described in note 21, as well to as anyone "reasonably suspected" of committing a terrorism offense or who is "knowing[ly] involve[ed]" with certain designated terrorist organizations or violent groups or of "being an agent of a foreign power." The latter two categories are not automatic exclusions, but HHS has the authority to limit or deny access to such agents and toxins if "determined appropriate by the Secretary, in consultation with the Attorney General." Sec. 351A(e)(2)(D).

[28] Information concerning the security risk assessment can be found at Federal Bureau of Investigation Web site, "Bioterrorism Risk Assessment Form and Instructions," http://www.fbi.gov/terrorinfo/bioterrorfd961.htm.

assessment provisions discourage qualified individuals from engaging in legitimate biological and agricultural research "because of the apparent infringement of these rules on individual liberties and the Fourth Amendment."[29]

While the government's response to bioterrorism to date has largely focused on enhancing the monitoring and control of biological research and materials, the continuing threat has also prompted calls for extending regulatory authorities both to suppress research and to respond to biological attacks. On the prevention side, proposals to restrict the flow of information—including controls on the publication of research papers, scientific conferences, and the sharing of information with foreign scientists—have raised serious concerns about the implications of bioterrorism policy for free speech and scientific advancement.[30] Meanwhile, proposals to increase the government's response capabilities—in particular proposals to broaden federal and state power to isolate and quarantine those who may have been infected by a contagious agents—would rely on the robust use of long-dormant detention powers in considerable tension with modern due process norms.[31]

The biotech industry is also beginning efforts at self-regulation. Gene synthesis companies that sell sequences of genetic material prepared to order have begun screening orders for sequences that match (or match significant fragments of) pathogens listed as select agents.[32] Some experts have proposed going further and actually building such screening mechanisms into gene synthesis equipment available to laboratories.[33]

In short, it's hard to imagine that someone could build a personal WMD arsenal without running afoul of numerous criminal laws and regulatory regimes—and various systems are either in place or being developed to flag bad actors before they strike. All that said, it's almost equally hard to imagine any of this deterring someone truly committed to launching a devastating attack, particularly if such a person lived or operated abroad. If the world makes it to 2025 without suffering a major non-natural biosecurity event, we will likely owe our good fortune not to either the lack of opportunity for individual or small-group mayhem but to a combination of a lack of imagination and a lack of technical sophistication on the part of the bad guys.

---

[29] National Research Council, *Biotechnology Research in an Age of Terrorism* (The National Academies Press, 2004), 44.

[30] Ibid.

[31] See Josh Gerstein, "Obama Team Mulls New Quarantine Regulations," *Politico*, August 5, 2009, http://www.politico.com/news/stories/0809/25814.html. See also *Notice for Proposed Rulemaking to amend CFR parts 70 and 71,* 70 Federal Regulation 71892-71948, Center for Disease Control and Prevention (November 30, 2005); Centers for Disease Control and Prevention Web site, "Public Responses to Proposed Regulations," http://www.cdc.gov/ncidod/dq/nprm/viewcomments.htm.

[32] See H. Bugl et al., "DNA Synthesis and Biological Security," *Nature Biotechnology* 25 (June 2007): 627-629; see also Jeremy Minshull and Ralf Wagner, "Preventing the Misuse Of Gene Synthesis," *Nature Biotechnology* 27 (September 2009): 800-01.

[33] Ali Nouri and C.F. Chyba, "Proliferation-Resistant Biotechnology: An Approach to Improve Biosecurity," *Nature Biotechnology* 27, no. 3 (March 2009): 234-36.

The Constitutional Stresses

If the threat landscape in the life sciences is really as terrifying as I have suggested, two conclusions almost certainly follow. The first is that government will act aggressively, either before a major event, after it, or both. It will act beforehand if it grows scared enough, if there are enough near-misses like the 2001 anthrax attacks to keep officials cognizant of the problem, and if it can generate the political will to support strong measures. It will act after the fact whether or not it acts before, because pressure on officials to do something will be inexorable. The polity in that context will almost certainly demand that officials *prevent* subsequent incidents, not merely that they respond better to future biosecurity events. As happened after September 11, a consensus will develop that retroactive actions—whether criminal prosecutions for terrorists or public health response to human-caused biosecurity crises—are simply inadequate and that government must stop future events before they happen in the first place.

The second conclusion is that faced with strong actions that stress constitutional norms, the courts will tend to uphold those that promise to work and strike down those that do not. Judges behave pragmatically, and the old saw that the Constitution is not a suicide pact will loom very large in the mind of any judge inclined to block enforcement of a policy that reasonably stands to prevent major bioterrorism events. Indeed, the doctrine itself already tends to reflect this pragmatism. The relevant constitutional tests will look at questions such as whether a given policy is narrowly tailored to achieve a compelling state interest or whether a policy uses the least restrictive means to achieve its goals. Under any such test, a policy that can plausibly be expected to have a significant impact on the problem is going to fare far better than one that seems like a stab in the dark.

This fact puts an enormous premium on the question of what policies, if any, are likely to prove effective in preventing, or effectively managing, biosecurity events. If some magic bullet policy with great capacity for prevention proved quite burdensome on someone's asserted constitutional rights, we could reasonably expect that this policy would both at some point be adopted and, the stakes being as high as they are, upheld—if not before the first major event, certainly after it. The trouble is that while many of the policy options push up against constitutional norms—either against existing doctrines or likely doctrines—none seems like much of a magic bullet. In the absence of judicial confidence in their success, it is clear neither that they will be sustained nor that they should be sustained. Rather, the range of possible responses includes many that will do little to prevent abuses while both abridging liberty and impairing the legitimate research that is key to finding cures and vaccines. To illustrate this point, let us consider several of those options in turn.

Restricting Research

The first, and perhaps the crudest, option is simply to ban certain categories of life sciences research—at least outside of the classified setting. Congress and the Executive Branch could take the position that certain research is so profoundly dangerous that it should not take place at all in the public domain. Rather, defensive research within this space should take place in classified laboratories, much as nuclear weapons research takes place at the national laboratories. And private individuals and companies, except under government supervision, shouldn't be the in the business of conducting such research at all. The idea here would be to stuff the genie back into the bottle—at least to a point—and to prevent further public breakthroughs from simplifying the bad guys' task.

This strategy seems to have both a bleak prospect of effectiveness and a high probability of gravely impairing a great deal of legitimate research. It is, after all, hard to come up with treatments for diseases without studying the agents that cause those diseases. Yet under this scheme, research on treatments for especially dangerous infectious agents would have to either take place in a classified setting or not at all. The result would likely be slower progress in developing vaccines and therapies for precisely the diseases about which authorities are most concerned. What's more, research restrictions would probably not impair those who would misuse biotechnology nearly as much as it would impair those who would use it for peaceful purposes. So much information is already public, and the materials are so widely available that it is implausible to imagine its stopping research by those who do not wish to be stopped. The old adage that if owning a gun is a crime, only criminals will have guns, is pointedly true of biotechnology research. If research on pathogens is discouraged or frustrated, the bad guys will be deterred far less than the good guys, and we'll probably have many fewer treatments both for naturally occurring and man-made outbreaks.

Given this reality, I suspect serious efforts to impede public biotechnology research will face serious obstacles in the courts—though no current doctrine would seem to preclude it. The Supreme Court has never held that scientific inquiry is protected by the Constitution.[34] Still, a substantial body of scholarship suggests on various different grounds, principally the First Amendment, that some degree of constitutional protection for scientific inquiry exists.[35] One can easily imagine judges deferring to reasonable regulations of research when those regulations are undertaken to protect public safety; this much is uncontroversial and such regulations are already in place. But it is quite a different matter to imagine that judges would sit still for grave limitations on free inquiry into human health—inquiry with the capacity to save many lives—in the pursuit of a policy

[34] The closest it has come is the dictum in *Griswold v. Connecticut* that "[t]he right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read a*nd freedom of inquiry, freedom of thought, and freedom to teach*. . . . Without those peripheral rights the specific rights would be less secure." See Griswold v. Connecticut, 381 U.S. 479 (1965).

[35] See, e.g., Steve Keane, "The Case Against Blanket First Amendment Protection of Scientific Research: Articulating a More Limited Scope of Protection" *Stanford Law Review* 59 (2006-2007): 505.

with such a limited probability of success. While no formal doctrinal bar to such a policy exists at present, I suspect the courts would erect one quickly in the absence of stronger reason than now exists to believe such a policy has any prospect for success.

In any event, except in perhaps the most targeted fashion, research restrictions would be a most foolish policy move. Biosecurity is a kind of arms race, in which the best hope for long-term security is good public health infrastructure combined with rapid progress in fighting infectious disease. Impeding that progress would be counterproductive in the extreme—even if preventing bioterrorism were the only biosecurity goal (which it is not).

Publication Restrictions

A somewhat less draconian option is to restrict publication of scientific papers that offer particularly useful guidance to would-be biological bad actors. Research would be permitted and regulated only as it is regulated now, but the government might seek to prevent publication of especially dangerous experiments.

Perhaps ironically, given that this approach is actually milder than the one described above, it is much more clearly problematic constitutionally under current doctrine. It is a commonplace that the First Amendment looks askance at prior restraints on speech, and that is the case even where the courts find credible the government's contentions that significant harm will follow publications.[36] In the modern era, it literally takes a publication's attempt to offer details on how to build a nuclear bomb to justify a prior restraint—and even in that case, the magazine in question eventually published.[37] In that instance, the publication offered nothing like the case a scientific journal could make regarding the value of the speech in question. After all, these articles are not, generally speaking, how-to manuals for catastrophes but serious science undertaken for altogether legitimate reasons. The terrifying mousepox study described above, for example, was aimed at improving methods of pest eradication. Other studies are efforts to understand and describe viruses, the better to attack them. There is serious social benefit to this work—benefit which the courts would rightly consider weighty.

What's more, in contrast to scientific research itself, there is little question at all that scientific *publications* are protected by the First Amendment. Steve Keane, who opposes constitutional protection for research, nonetheless acknowledges that "scientific expression," which "includes scientific publishing and communication . . . is entitled to normal free speech protection. In fact, the Supreme Court and lower courts have repeatedly indicated, in dicta, that scientific works and scientific expression are protected by the First Amendment."[38]

Almost nobody contends that no life-sciences research should be withheld

[36] See New York Times Co. v. United States, 403 U.S. 713 (1971).
[37] United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979).
[38] Keane, *supra* note 32 at 508.

from the public on safety grounds. In the wake of September 11, facing criticism for some of the studies they had published and calls for greater oversight and regulation, medical and scientific journals began developing procedures to consider the safety implications of research publications in the life sciences.[39] In a joint statement of principles published in 2003, the editors of several leading journals acknowledged that "on occasions, an editor may conclude that the potential harm of publication outweighs the potential society benefits. Under such circumstances, the paper should be modified, or not published."[40] But this sort of self-regulation is a far cry from government censorship. And it is reasonable to expect the courts to treat censorship with a great deal of skepticism.

In a provocative article on what he terms "crime-facilitating speech," Eugene Volokh proposes that speech ought not be constitutionally protected when "it can cause extraordinarily serious harm (on the order of a nuclear attack or a plague) even when it's also valuable for lawful purposes."[41] This sort of thinking offers a potential doctrinal path for a court inclined to uphold publication restrictions, should the government ultimately go that route. But again, the question of the effectiveness of publication regulation will—and probably should—loom large in any adjudication. Unless there is compelling reason to believe that publication could bring about a catastrophe, and that stopping publication will avert it, courts have enormous doctrinal momentum in the direction of ensuring press freedom.

Publication restrictions, particularly if highly targeted, stand a better chance of at least limited effectiveness than restrictions on the underlying research itself. One could imagine how a system of screening papers before publication might keep particularly dangerous material out of the public domain and perhaps divert publication into classified settings. This would function much like the self-regulatory system the journals have already created, except with a security officer, not an editor, making the final call as to whether a given paper would require modification or non-publication.

But its effectiveness would likely be quite limited, and it's not at all clear that such a system would impair the bad guys more than it would frustrate the good guys. Foreign journals would probably publish papers banned from publication in the United States. And in any event, scientists have many means other than paper publication—conferences, seminars, emails, informal conversations, and blogs, for example—of sharing results and methods. In any event, such a system would do nothing to prevent people from using the huge wealth of information already public for evil purposes. Quite apart from such a system's being repugnant to First Amendment values, in other words, it would be far from a silver bullet.

---

[39] See National Research Council, Biotechnology Research in an Age of Terrorism, (National Academies Press, 2004), 96-99.

[40] Ibid., 99.

[41] Eugene Volokh, "Crime-Facilitating Speech," *Stanford Law Review* 57 (2004-2005): 1106.

Licensing, Registration, Surveillance, and Data Mining

A more promising avenue, both in terms of effectiveness and in terms of constitutional plausibility, is to focus not on restricting research or publication but on monitoring the use of gene synthesis equipment and the companies and scientists who employ them. The simplest and perhaps most effective strategy in this regard may simply be to require a license before permitting certain categories of genetic research and experimentation. One needs a license to operate an amateur radio; it hardly seems onerous to suggest that one should need one to meddle in genetics. Licensing would give government a window into who is working with what. It would also allow the criminalization of a wide range of unauthorized activity. It would not, of course, prevent that unauthorized activity. People drive without licenses, and those who want to build bugs will do so without licenses too. But it does offer a mechanism of governmental leverage and monitoring.

Along related lines, the major gene–synthesis companies, which sell gene sequences by mail-, phone-, and Internet-order, now screen orders for sequences associated with "select agents and toxins" listed under the 2002 Bioterrorism Response Act and refuse to sell such sequences to those who are not registered under that Act.[42] At least in theory, this should prevent a bad actor from buying, say, the smallpox virus genome or buying sizable segments of it and then assembling them in his own laboratory. Yet this system would do nothing to prevent that same bad actor from building the sequence himself or modifying a related one to match it. In an article published early in 2009, Ali Nouri and Christopher Chyba proposed building the existing screening system directly into the gene synthesis equipment that is common in many labs. Manufacturers would program the computers that drive the machines to decline to produce select-agent components unless the user were registered to work with them. The software, in this proposal, could automatically update its list of prohibited sequences much the way antivirus software updates the list of malware it identifies and purges.[43] The proposal, vaguely reminiscent of proposals during the 1990s to require back-door access for law enforcement to encryption systems, drew a sharp response from biotech executives that was similarly reminiscent of the attacks on the so-called Clipper Chip and other key escrow encryption schemes.[44]

As it stands now, the screenings system—and probably even Nouri and Chyba's proposed enhancement of it—would be more of an inconvenience to a biohacker than a true prevention mechanism. It might force a bad actor to use older technology that predates the embedded screening systems or to use sequences brief enough not to trigger the screening system. People would surely

[42] See H. Bugl et al., "DNA Synthesis and Biological Security," *Nature Biotechnology* 25 (June 2007): 627-629; see also Jeremy Minshull and Ralf Wagner, "Preventing the Misuse of Gene Synthesis," *Nature Biotechnology* 27 (September 2009): 800-01.
[43] Ali Nouri and C.F. Chyba, "Proliferation-Resistant Biotechnology: An Approach to Improve Biosecurity," *Nature Biotechnology* 27, no. 3 (March 2009): 234.
[44] See Minshull & Wagner, *supra* note 39.

seek to hack the system and disable the screening software. And it would do little to prevent modification of existing DNA sequences. Someone truly committed and technically capable would find a way around it—though it may well stop low-grade amateurs and it should make any bad actor's life at least a bit more difficult.

The system, however, would have an obvious set of legal advantages—namely that it seems to raise no particular constitutional difficulty. There is, after all, no constitutional right to create pathogens, or to privacy in one's pathogenic experimentations. What's more, one can imagine further developments of the technology that would make it far more robust as a prevention tool. What if gene-synthesis equipment alerted authorities whenever an unauthorized person tried to create a proscribed sequence? More intrusively, what if the equipment reported constantly on its own activities, so that authorities would have an ongoing data stream that enabled them to monitor who was creating what gene sequences? If one takes seriously the notion that there is no right to privacy in genetic engineering experimentation, there ought to be no constitutional obstacle to such a requirement—though there would surely be strong policy objections to government's engaging in constant surveillance of research.

Major hurdles remain to developing this area, not the least of which is creating enough international uniformity that bad actors don't simply buy and use their equipment in countries that don't require embedded surveillance systems. That said, this area represents a relatively promising avenue for policymakers who are seeking a robust tool for preventing man-made biosecurity disasters.

The trouble arises from the fact that to be truly useful, the data from such a system would likely have to be analyzed in conjunction with other data. It is, after all, far less threatening to know that Scientist A is manipulating fragments of DNA from an infectious agent if one also knows that he has published extensively on the treatment of that agent than, say, if he has recently purchased copies of the *Turner Diaries* and is a member of the Aryan Nations. This raises the larger question of data-mining in a particularly troubling form: surveillance of science leading to ongoing data-mining of individuals against whom government has no individualized suspicion. In other words, the government would be essentially asserting the right to conduct ongoing background checks against anyone involved in the life sciences.

In one sense, of course, this merely builds on the current system of background checks for those registering under the 2002 Bioterrorism Response Act to handle select agents—risk assessments (essentially background checks) that already allow the FBI to query databases and other agencies to flag those ineligible to register. As in those background checks, the hit rate would be miniscule. In 2009 congressional testimony, an FBI official stated that "Since the inception of the [Bioterrorism Risk Assessment] program, [it] has completed 32,742 [background investigations]. Two hundred and eight individuals have been restricted"[45]—a hit rate of approximately

[45] *Testimony of Daniel D. Roberts, Assistant Director Criminal Justice Information Services Division Federal Bureau of Investigation, Hearing on Strengthening Security and Oversight at Biological Research Laboratories, Senate Judiciary*

six thousandths of one percent. So the program would operate as a huge fishing expedition looking for anomalies in scientific behavior.

Exactly how troubling this would be would depend, to a great degree, on who looks at what data, when, and with what degree of cause. Currently, the constitutional landscape for data-mining is relatively permissive. Much data the government might choose to examine is not plausibly within the ambit of the Fourth Amendment as currently interpreted, and in any event, Fourth Amendment law has an exception allowing warrantless searches for "heavily regulated industries"—of which at least some biotechnology labs probably qualify.[46]

My guess is that the combination of licensing, technological blocking of select-agent production, monitoring of the use of gene-synthesis equipment, and examination of data relevant to people whose use of this equipment raises red flags probably represents the most promising policy avenue in the prevention department. Done right, it stands to minimally impact ongoing science; as long as people are entitled to use their equipment for the purpose they deploy it, after all, it would do nothing more than create an audit trail. While more than a little creepy, it faces no greater constitutional barrier than, say, running data checks on people who get on airplanes. And it stands to provide a real-time stream of data about who is using what equipment to make what genetic sequences—data that could tip off investigators at a relatively early stage of a developing biosecurity disaster.

That said, it is far from a cure-all. If the embedded technology is not mandatory, it could simply drive a market for surveillance-free gene synthesis equipment—much the way the voluntary key escrow policy in encryption led to widespread adoption of non-key-escrow encryption algorithms. If other countries don't adopt the same standard, an American policy requiring such technology could also simply create incentives for companies to move biotechnology work overseas or to use foreign surveillance-free technologies. Finally, even imagining a perfect system, its coverage would be far less than 100 percent. Someone will successfully hack it and override its reporting and blocking functions. Someone else will figure out how to game the system so that his malicious conduct will not raise red flags with authorities. Computer security systems always fail eventually. This will be no exception.

Isolation and Quarantine

Finally, it's worth saying a brief word about isolation and quarantine, which have no capacity to prevent a biosecurity event but might under some circumstances be key to managing one. In the context of any major biosecurity event, particularly one involving a highly contagious and lethal pathogen, the question of isolation will inevitably arise. The power of quarantine and isolation is traditionally broad,

Committee, Subcommittee on Terrorism and Homeland Security, September 22, 2009, available at .

[46] New York v. Burger, 482 U.S. 691 (1987).

and quarantine laws have been upheld by the courts on public safety grounds in the past. But they have also not been used aggressively in decades, and across many other areas, governmental powers to detain people outside of the criminal justice apparatus is on the wane. Over the past ten years alone, for example, the power to detain the enemy in wartime—at least when the enemy is out of uniform and difficult to identify clearly—has come under sustained challenge, and the courts have imposed significant new review mechanisms. They have done this notwithstanding relatively clear doctrine that seemed to establish that habeas corpus review was not available to the alien detained overseas—doctrine in which the government had a surpassing reliance interest.[47] The Supreme Court has similarly shifted the landscape of allowable immigration detention.[48] One can probably expect, therefore, that quarantine laws—which involve minimal due process before permitting detention—will face significant constitutional challenge as well if used aggressively. And while authorities have apparently strong precedents that permit aggressive quarantine and isolation policies, they would do well not to assume that those precedents will have staying power.

As this brief overview makes clear, the possible impact of these technologies—and the government's response to them—on the Bill of Rights could range significantly. If one imagines that courts see promise in muscular government actions, the impact could be quite profound—the development of doctrine affirmatively tolerating limitations on research, publication of research, real-time surveillance of biomedical science and scientists, and a renewal of a long-dormant tolerance for detaining sick people. By contrast, if one imagines that the courts will respond to strong countermeasures as ineffective shots in the dark that offend basic values, one could imagine litigation's clarifying doctrine in the opposite direction in many of these areas, leaving government with few tools to address a profound security problem. The striking fact, is that—save for significant investment in biomedical research—there exists no policy option that is both likely to be especially effective and poses no serious doctrinal question.

The Biggest Impact?

This lack of promising, clearly constitutional options—or even promising *unconstitutional* options—gives rise to what I suspect will be the most profound impact of this class of technologies on the Constitution. Ironically, the impact will not be felt on the Bill of Rights but on the very structural arrangements of power the core document contemplates. That is, it stands to bring about a substantial erosion of the government's monopoly on security policy, putting in diffuse and private hands for the first time responsibility for protecting the nation.

There are people who would write that sentence with joy in their hearts. I am not one of them. My views on executive power—notwithstanding the excesses of

[47] Boumediene v. Bush, 553 U.S. 723 (2008).
[48] See Zadvydas v. Davis, 533 U.S. 678 (2001); see also Clark v. Martinez, 543 U.S. 371 (2005).

the Bush administration—are unapologetically Hamiltonian. The constitutional assumption that the political branches, particularly the executive branch, are both responsible for national security and have the tools necessary to fulfill that responsibility is a comforting one, the destabilization of which I find scary. "Power to the people!" is a slogan that has always rung to me of gridlock at best, mob rule at worst.

The Constitution contains very few textual exceptions to the notion that national security is a federal responsibility. One, the Second Amendment, embodies the Framers' reverence for state militias, both as a means of fending off native attacks and as a means of preventing federal encroachments on state prerogatives. The other, the Letters Marque Clause of Article I, contemplates a limited role for the private sector in military engagements—under congressional supervision.[49] Both involve institutions that have long since lapsed into disuse. The broader and more lasting presumptions were that Congress would make the rules of security and that the President would lead the armed forces and the larger executive apparatus in a military or other crisis.

I'm not sure how these presumptions hold in the face of rapid development of these technologies. This point is perhaps most vivid in the cyber arena, where a huge amount of traffic into and out of the United States—including government traffic—now takes place over privately owned lines and the government quite literally does not control the channels through which attacks can occur. But it's also true in the biotechnology sphere. Because the revolution has taken place largely in private, not government, hands, the government employs only a fraction of the capable individuals. And the capacity to respond to or to prevent an attack is therefore as diffuse as the capacity to launch one.

This point is crucial and provides the only real ray of hope in an otherwise bleak picture. The biotechnology revolution has given enormous numbers of people the capacity to do great harm, but it has also given enormous numbers of people the capacity to work to prevent that harm. The proliferation of defensive capability has been as rapid as the proliferation of offensive capability—only exponentially more so since the good guys so vastly outnumber the bad guys. The individual scientist had no ability to prevent the Soviet Union from launching a nuclear attack against the United States or invading Western Europe. But the individual scientist, and groupings of individual scientists, have an enormous role in biosecurity—from driving the further innovations that can wipe out infectious diseases, to spotting the security implications of new research, to reporting on colleagues engaged in suspicious activities out of sight of authorities. The policies of universities thus take on security importance, as do the postures of private companies and the research agendas of individuals. The number of actors capable of playing a significant role in the solution grows as quickly as the number of people capable of creating the problem.

This fact will, I suspect, tend to force changes in the constitutional structures of

[49] U.S. Constitution, art. 1, § 8, cl. 11.

security. I don't mean here that any kind of formal doctrinal shift will take place. The change will be far subtler than that. The point is that as the powers the Constitution grants to government actors grow less plausible as tools for the problems they confront, the Hamiltonian executive—capable of strong decisive action characterized by secrecy and dispatch and energy—will be of more limited use. Going after a multiplicity of dangerous actors authorities cannot identify using facilities the government neither own nor controls in locations over which it may have no jurisdiction will not flatter the Hamiltonian executive. The Congress charged with creating rules for that executive is positioned little better. And so aspects of our security policy will tend to devolve to those actors better positioned to have real impact.

Changes to the nature of the executive in response to shifting circumstances and in the absence of major doctrinal movement are far from unheard-of in American history. The Founding Era presidency was tiny. Yet as the need for the regulatory state grew during the New Deal and World War II, it ballooned into the behemoth of the Imperial Presidency. This change, of course, involved some degree of doctrinal change, but surprisingly little—Article II of the Constitution being ultimately consistent both with a small streamlined presidency and with a giant federal bureaucracy. This period saw huge doctrinal changes in the substantive scope of federal power, but the presidency itself changed largely by ongoing adaptation—by growing in response to perceived need.

The change in response to this problem will probably be similar. Nobody's going to rewrite the Constitution or, more plausibly, rethink constitutional doctrine to vest security responsibility in non-governmental actors. It will just happen. As government finds itself relatively feckless in the face of the problem and other actors find themselves capable of responding, we will start thinking about those other actors as bearing important security functions for which we once looked to government. And government itself will end up playing, I suspect, more of a coordinating function with respect to these other actors than the classical defend-the-borders model of security.

Curiously, and more than a bit ironically, this fact pulls the mind back towards themes and ideas eloquently articulated by scholars such as James Boyle and Laurence Lessig in the context of the debate over intellectual property. A major current of this body of thought involves the protection of legal space for communities of various sorts to use and borrow one another's ideas and work in collaborative efforts to build things. Boyle's recent book, for example, contains a spirited defense of distributed applications like file sharing, of the open-source software movement, and of Creative Commons licenses.[50] Indeed, the world has seen amazing demonstrations of what large groups of people can do when they pool expertise—even with very limited coordination. The most famous example is Wikipedia, but this is far from the only one. Anyone who has used Open Office—an open source alternative to the Windows Office application suite—knows that it

[50] James Boyle, *The Public Domain: Enclosing the Commons of the Mind*, (Yale University Press, 2008), 179-204.

doesn't take a major software company to produce a major piece of software. It is an interesting fact, highly salient for our purposes here, that open-source software is often more stable and secure than proprietary code.[51] While this point has its dissenters, the famous line in the open-source software movement that "given enough eyeballs, all bugs are shallow" may have real application not just to computer bugs but to biological ones as well.[52]

Given that security will be, to borrow a term from this lexicon, a more distributed application than it has been in the past, we ought to start thinking about it as such. And here the landscape actually seems somewhat promising. There are, as I have noted, many more good guys than bad guys in the biotech world. They are enormously innovative. And they are much closer to the ground than is government. They offer a great deal of capacity to identify the bad guys and to develop countermeasures to their actions—a huge reservoir of thought and expertise in the development both of strategies for responses and prevention.

It's hard to envision the long-term migration of the defense function in any detail; it is not hard, however, to envision various iterations of biosecurity as a distributed application with government functioning more as a coordinating mechanism than as front-line defender of the nation. At the most basic level, for example, government can create a favorable environment for the sort of biotech research that will help win the arms race against biosecurity malefactors. Government can identify treating infectious disease as a major national research and funding priority. Putting a large amount of money behind basic research, behind the development of new therapies and vaccines, and behind the improvement of response times to new outbreaks would create a major incentive for industry and university researchers to innovate faster than the relatively small number of bad guys do. The more people one can muster in this direction, the greater the numerical advantage in brain power the good guys can deploy, the greater the likelihood that cures and treatments will outpace manufactured (and natural) diseases. This has already happened to a considerable degree, particularly since September 11. But there's a lot more government can do in the way both of conceiving of infectious disease research as a national-security strategy and in creating a favorable research, regulatory, and liability environment in which to improve capacity to defeat infectious agents. Any such approach would—indeed does—involve government's setting of priorities and funding security work but not directly conducting the activity that may be central to long-term security. That work, rather, is broadly distributed to a research community incentivized to address a security function that the government itself is ill-positioned to confront.

Second, while government cannot monitor all biotech research, biotech researchers can more effectively monitor one another and might—under the right circumstances—serve as a network of security eyes and ears. Efforts to harness the

[51] Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*, (John Wiley & Sons, 2000), 343-45.
[52] Eric Raymond, "The Cathedral and the Bazaar," available at http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/ar01s04.html.

public to the project of security have not always fared well. The Bush Administration's ill-fated TIPPS program, an effort to get people to report suspicious activity, came off as a Big Brotheresque spying program. But large numbers of humans offer some of the strongest, most flexible security there is, and a culture in which researchers know what one another are working on and have the instinct to raise questions about oddities is a more secure culture than one in which people work in vacuums and keep their mouths shut. While enormous cultural obstacles in the scientific community currently impede the development of a more secure culture, somehow, we will ultimately have to mine the now-latent protective potential of a crowd of highly educated people up close to the process.

Third, one can imagine various technological devices by which users might take greater responsibility for the security of the biotech platform. Some of the screening technologies discussed above, for example, could become helpfully ubiquitous if, say, university and industry policies strongly militated towards their use. Government may have a regulatory role here in encouraging both the development and the deployment of such technologies, but again, the front-line defense will necessarily be distributed among the thousands of people working in biotech. Similarly, as biotechnology moves away from artisanal crafting of unique sequences towards more standardized constructions of genetic materials out of what are essentially microscopic Legos, one can imagine tagging those Legos with identifying information—which could potentially make attribution of misconduct far easier. Most color laser printers leave information on every copy they make that identifies the specific equipment that produced the copy, an effort to prevent counterfeiting. A strong norm towards the embedding of tracing information in the constituent elements of bioengineered sequences could be key to knowing who is producing what—or at least to being able to figure out in retrospect from where bad things came.

Finally, people in universities and industries need to feel themselves to have a security function. When I was a child in New York City in the 1970s, I was crossing Columbus Avenue with my father—with whom I had just been playing baseball in Central Park. As we were crossing the street, a young man snatched the purse of an older woman crossing towards us and sprinted northward up the street. The woman yelled, and spontaneously and with no coordination, half a dozen—maybe ten—men in the immediate vicinity (my father among them) sprinted after him. They ran him down ten blocks later and held him until the police arrived. This is distributed security in the absence of a strong executive presence. There are enormous obstacles to the development of such a model globally across complex technological platforms. One of the most daunting is the culture of the scientific community, which does not tend to think in security terms. That said, it may be a vision of our technological and constitutional future—as well as a memory from my past.

The author gratefully acknowledges the excellent research assistance on this project of Rhett P. Martin and Rabea Benhalim and the extraordinarily helpful comments and technical guidance of Roger Brent.

Benjamin Wittes is a senior fellow in Governance Studies at The Brookings Institution. He is the author of Detention and Denial: The Case for Candor After Guantanamo, forthcoming from the Brookings Institution Press. He is also the author of Law and the Long War: The Future of Justice in the Age of Terror, published in June 2008 by The Penguin Press, and the editor of the 2009 Brookings book, Legislating the War on Terror: An Agenda for Reform. He co-founded and co-writes the Lawfare blog (http://www.lawfareblog.com/), which is devoted to non-ideological discussion of the "Hard National Security Choices," and is a member of the Hoover Institution's Task Force on National Security and Law.

His previous books include *Starr: A Reassessment*, which was published in 2002 by Yale University Press, and *Confirmation Wars: Preserving Independent Courts in Angry Times*, published in 2006 by Rowman & Littlefield and the Hoover Institution.

Between 1997 and 2006, he served as an editorial writer for *The Washington Post* specializing in legal affairs. Before joining the editorial page staff of *The Washington Post*, Wittes covered the Justice Department and federal regulatory agencies as a reporter and news editor at *Legal Times*. His writing has also appeared in a wide range of journals and magazines, including *Slate*, *The New Republic*, *The Wilson Quarterly*, *The Weekly Standard*, *Policy Review*, and *First Things*.

Benjamin Wittes was born November 5, 1969 in Boston, Massachusetts, and graduated from Oberlin College in 1990. He recently earned a black belt in taekwondo.

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
www.brookings.edu/governance.aspx

Editor
Jeffrey Rosen
Benjamin Wittes

Production & Layout
John S Seo

E-mail your comments to gscomments@brookings.edu