SKATING ON STILTS

Why We Aren't Stopping Tomorrow's Terrorism

Stewart A. Baker

HOOVER INSTITUTION PRESS
Stanford University Stanford, California

12 Smallpox in the Garage

In January 1970, a German electrician fell ill after a trip to Pakistan. He was hospitalized with what appeared to be typhoid fever. He had been isolated for several days when the doctors realized that he didn't have typhoid fever.

It was smallpox.

Fear riffled through the hospital, and the community beyond. Smallpox has probably killed more human beings than any other disease. And it kills them with particular cruelty. After starting out like a bad flu, after a few days the disease attacks the victim's skin. Tiny spots appear, spread, and then harden into pus-filled blisters. Gradually, with excruciating pain, the blisters pull the outer layer of skin away from the under-layers. Sometimes the skin pulls loose in sheets. Sometimes the blisters attack not just the skin but the eyes, the throat, and every other orifice, ripping loose skin inside the body as well. Desperate with thirst, the victims can't drink; swallowing is just too painful.

Throughout it all, the victim remains fully conscious. A third or more of the victims die. Those who survive are often permanently scarred, or blind or both.

The electrician lived. But many who came into contact with him were infected. Several died.

What was most frightening was how the virus spread. One victim spent only fifteen minutes in the hospital. All he did was ask directions, briefly opening a door that led to a corridor thirty feet from the patient's room. That was enough. He came down with smallpox.

Three other victims were even farther away—two floors above the electrician's isolation ward. It was January, but tests revealed that opening the hospital windows just a crack allowed currents of air to drift between rooms on different floors. The virus had floated out the patient's window and along the outside wall; it then slipped into three different rooms two stories above, infecting patients in each room.

Seven years later, in 1977, Ali Maow Maalin also fell ill with smallpox. This time, though, it turned out to be good news.

Maalin was a cook from Merca, Somalia—where smallpox was making its last stand. Vaccination was slowly tightening a noose around the disease. Because smallpox reproduces only in humans, widespread vaccination left fewer and fewer places for the virus to reproduce and spread.

The first vaccination for smallpox—or indeed for any disease—came in 1796. That was when Edward Jenner realized that milkmaids who caught cowpox seemed to be protected from smallpox, to which cowpox was related. Jenner's vaccine based on cowpox marked the beginning of man's counterattack on smallpox. By the 1970s, vaccinations had gradually reduced the disease's natural range to the wilds of Somalia and Ethiopia.

The World Health Organization hoped to make Ali Maow Maalin the last victim of smallpox in history. It quickly vaccinated everyone who had been in contact with him, then held its breath. Would other cases flare up?

WHO waited.

A year.

Two years.

Three.

At last, after three years with no natural cases of smallpox, the World Health Assembly declared victory. It triumphantly called a special 1980 meeting.

"[T]he world and all its peoples have won freedom from smallpox," the assembly declared. This was "an unprecedented achievement

in the history of public health." Together, the nations of the assembly had "freed mankind of this ancient scourge."[1]

Copies of the virus were locked away in Atlanta and Moscow for research purposes, but the disease was gone from nature. Vaccinations stopped. Few Americans born after the 1960s have the dimpled scar on their arm that is the last trace of mankind's worst nightmare.

It had taken a bit less than two centuries for vaccination to free the world from "this ancient scourge."

Today, the likelihood that the world will remain free from this ancient scourge is close to zero.

Smallpox is back, or nearly so.

Within ten years, any competent biologist with a good lab and up-to-date DNA synthesis skills will be able to recreate the smallpox virus from scratch. Millions of people will have it in their power to waft this cruel death into the air, where it can feed on a world that has given up its immunity.

How can I be so sure? Easy. I've seen the same thing happen already, and so have you. The very same revolution that made possible the explosion of information technology—and set the table for network attacks—is now transforming biology, with consequences that are both exalting and frightening.

The same relentlessly exponential improvement in technology that gave us Moore's Law and that democratized the computer is now democratizing the technology of life. It is empowering an army of biologists to tinker with biology in ways that will help us all live longer and more comfortable lives.

And then, unless we do something, it will kill us in great numbers.

"Synthetic biology" blends biology, chemistry, and engineering. The field really began to take off when it moved from laboriously replacing a single gene to building whole stretches of the genome from scratch.

DNA is organized like a spiral staircase, and each step on the stairs is called a base pair. Linking base pairs together into longer sequences

allows researchers to make more complex genes—and ultimately more complex organisms. So progress in synthetic DNA is measured by how many base pairs have been successfully strung together. In recent years, progress has been exponential.

In 2002, after a two-year effort, a team of researchers announced that they had assembled the entire polio virus. To do that, the team had to assemble 7,500 base pairs of DNA, precisely in order. The next year, scientists managed to knock years off the process, assembling a bacteriophage with 5,300 base pairs in just two weeks.

Two years later, in 2005, researchers' capabilities had tripled. A team managed to synthesize an influenza virus with 14,000 base pairs. Just a year later, they had surpassed that mark by a factor of ten, synthesizing the Epstein-Barr virus, with 170,000 base pairs.

Smallpox has 180,000.

By 2005, whether smallpox would be synthesized was simply a matter of choice, not of capability.

The following year, the outgoing secretary general of the United Nations, Kofi Annan, grew alarmed. He pointed to researchers' successes in building an entire virus from scratch and said, "In the right hands, and with the appropriate safety precautions, these are sound scientific endeavours that increase our knowledge of viruses. But if they fall into the wrong hands, they could be catastrophic." [2]

Too late. By 2009, the state of the art had left 180,000 base pairs in the dust. A team of researchers announced that it had assembled a bacterial genome with 583,000 base pairs. Creating smallpox from scratch was no longer even an interesting challenge.

Nor were these capabilities confined to a few specialty laboratories. Foundries sprang up to sell made-to-measure DNA, at ever-declining prices that put Moore's Law to shame. Synthesizing DNA cost $10 per base pair when George W. Bush ran for president in 2000. By the time of his second inauguration, the price was $2 per base pair. When he left office in 2009, the price was down to about 25 cents. For those who don't want to use a foundry, DNA synthesizers are available for sale on eBay.

Kofi Annan was wrong. This technology isn't going to fall into the wrong hands. Just like jet travel and powerful computers, it's going to fall into *everybody's* hands. The Mayo Clinic. Hezbollah. Pfizer. Al Qaeda. Apple. Ted Kaczynski, Timothy McVeigh, and the Fort Hood shooter.

They won't need their own labs to build bugs to order. Even today, it's possible to obtain long sequences of synthetic DNA simply by sending a message to the private "foundries" that assemble DNA to order.

Struggling to survive in a new market with thin margins, the foundries' sense of responsibility for what they make is, well, limited. The *Guardian* newspaper in Great Britain demonstrated this when one of its journalists successfully ordered a lightly modified piece of the smallpox genome over the web. The order was mailed to his home, no questions asked. When a dozen foundries were asked whether they screened DNA orders to see whether they were providing sequences that terrorists could turn into weapons, only five answered "yes."

As many as half the foundries questioned by journalists did not routinely screen their orders to make sure that they were not helping terrorists construct a dangerous virus. The order came in, and they filled it, often with no questions asked.

If current trends continue, anyone who can get his hands on a computer virus today will soon be able to get his hands on a custom-built biological virus.

And who can get his hands on a computer virus today? In an age of drop-down-menu malware attacks, the answer is simple.

Anyone who wants to.

Perhaps it isn't completely fair to assume that exponential growth in biotechnology will democratize biological terror in the same way that computer technology democratized computer crime. After all, unlike computer hackers, bio-hackers can't pretend that releasing pathogens is a good way to demonstrate their skills or to dramatize the need for better biosecurity. So perhaps biological malware will arrive more slowly than its computer counterpart. That's good.

So far, the terrorists who've tried to use biological weapons have turned out to be more hapless than terrifying. A cult that wanted to win an election in rural Oregon poisoned the local salad bar to suppress turnout. A Japanese group experimented with anthrax and ended up spreading a harmless, non-virulent vaccine strain around Tokyo. The anthrax-laced letters sent to prominent journalists and politicians in 2001 included a warning to take antibiotics and thus dramatically reduced casualties. Al Qaeda tried to acquire biological weapons before 9/11, but its efforts never really got off the ground.

Maybe large-scale bioterrorism is harder than it seems. Or maybe we're just in that golden era we also experienced in computer technology; maybe the bad news just hasn't caught up with the good news. Much the same thing happened with jet travel for that matter. Apart from some Brazilian military officers who commandeered a civilian flight in 1959 to further their coup attempt, there were no notable hijackings of a commercial flight before 1968, even though they had been possible since at least the 1950s. Early that year, though, an El Al plane was seized by Palestinian terrorists and a U.S. flight was hijacked and diverted to Cuba. Then the deluge began. By the end of 1968, there had been half a dozen hijackings to Cuba alone, and the stage was set for decades of ever more spectacular hijackings.

The lag between good news and bad owes something to the surprisingly conservative nature of terrorism. Terrorists don't like to fail; failure doesn't inspire fear. But once a new tactic has been pioneered, and it has become clear that governments don't know how to respond to it, everyone piles on. Suicide bombings were virtually unknown until the early 1980s, when they were used in the Lebanese and Sri Lankan conflicts. The tactic is now widely used by terror groups in many countries. We may be only one or two successful attacks away from a similar wave of bioterrorism.

When those attacks will occur, however, is anyone's guess. All we can say is that every year biological attacks become more probable, just as biotechnology becomes ever more democratized. And, of course, if disaster becomes more probable every year, then sooner or

later disaster will happen, though it may show up late. That's a lesson financial markets learned again in 2008 (as did New Orleans residents in 2005). Sooner or later, the inevitable does happen.

One cabinet-rank official summed it up a little differently after I gave him a briefing on the topic.

"Maybe," he said, "the human race isn't meant to survive."

I understood how bad the threat was. I had been briefed on it while investigating U.S. intelligence agencies' work on Iraq's WMD program. The agencies were eager to tell us how much they knew about other nations' nuclear weapons programs. We got briefing after briefing. Nukes were a major concern, and the agencies had scored many successes in penetrating other nations' programs.

On biological weapons, the intelligence community was noticeably less voluble. Everyone acknowledged that biological weapons were a terrible threat. Worse than nuclear weapons in some ways. They could kill as many people. And the aftermath would be worse. The day after a nuclear weapon goes off in an American city, a hundred nations will order their airlines to fly to the United States, carrying assistance until the crisis has passed. The day after a biological weapon is used in an American city, a hundred nations will order their airlines to stop flying to the United States until the crisis has passed.

But, with a few exceptions, intelligence operatives and analysts seemed almost to have lost hope of understanding other nations' biological weapons programs. The programs are easier to hide and require less in the way of investment than nuclear weapons. The equipment and training that supports them have many innocent commercial uses in the pharmaceutical and pesticide industries.

And the agencies' track records were not good. The Soviet Union—and Russia thereafter—had maintained a truly loathsome biological weapons program for decades after the United States gave up its program. It treated the disappearance of smallpox, and the worldwide end of smallpox vaccinations, as an invitation to devise more potent weapons using its stores of the pathogen. The Soviet program was

discovered only when defectors began to talk about their work on artificial new diseases that were proof against existing countermeasures, or that responded to treatment by changing into something even worse.

The same was true in Iraq. Saddam Hussein maintained a biological weapons program for years, hidden from both U.S. intelligence and UN inspectors. (If you're wondering why no such program was found after the U.S. invasion, the answer is that Saddam Hussein finally dismantled the program after his son-in-law defected and disclosed it to the West in 1995. Saddam admitted the existence of the program and announced that it had been shut down; intelligence agencies, shocked by what they had missed, credited Saddam's admission but doubted his claim that the easy-to-hide program had ended.)

Intelligence gaps on biological weapons raised our concern about anonymous attacks. Like computer malware, biological agents are hard to tie back to an individual or group. Ambiguity about attribution has already prevented the United States from taking effective retaliatory action against computer attackers. It's quite possible that we won't do any better against attackers armed with biological weapons. The best test of our capabilities came in the 2001 anthrax attacks. The FBI used great ingenuity and massive resources to question, search, and investigate all the likely suspects. It finally announced, to some skepticism, that it had identified the guilty man in 2008—seven years after the attack.

When I got to DHS, I asked my staff what we could do to cut the risk of biological terrorism. They described two new programs launched after the 2001 anthrax attacks. The first was to develop countermeasures—vaccines, treatments, etc.—for the most threatening pathogens. The second was to get a better picture of who actually had access to such pathogens inside the United States. These were large programs, funded by a Congress that feared another attack was imminent. But as the years went by without an attack, the programs had slowly been bent to fit the institutional inclinations of the agencies that got the money.

Take the countermeasures program. This is an absolutely essential step. Unlike nuclear weapons, biological weapons can be defeated even after the attack. That is, if we have a smallpox vaccine and can distribute it quickly, we can stop an infection in its tracks, greatly limiting the harm done by the disease. We could take the weapon out of terrorists' hands. A biological attack that is met by quick, effective countermeasures is like a bomb that has been defused before the blast.

But our countermeasures strategy has serious flaws. It requires a massive investment in medicines that often have no civilian use. We will never have a need for smallpox vaccine except to defend ourselves against attack. The doctors and researchers of the National Institutes of Health (NIH) were not used to battling human adversaries. They were scientists who wanted to do pure research, not something that felt like military work. Like any industry facing a market change, the traditional research community resented the funding that went to countermeasures research, and they didn't have much trouble turning that resentment into an ideological and personal campaign against the program. (The debate broke into the open when traditional NIH researchers launched a smear campaign against Tara O'Toole, the Obama administration's nominee to head DHS's science office. Her success at building a countermeasures research program led to her being labeled an alarmist and a female Dr. Strangelove by traditional researchers, delaying her confirmation for months.)

More troubling was the way business as usual in other parts of the Department of Health and Human Services threatened our ability to actually use the countermeasures that had been developed at such great cost. For example, getting approval for such countermeasures is staggeringly expensive. A host of regulatory hurdles has been set up for new drugs. The regulations assume that the drugs are being championed by private companies hoping to make billions in profits if they are approved. But the private sector will not spend billions to get regulatory approval for a product that may never be deployed.

Even if government pays that cost, most countermeasures, such as vaccines, have side effects that may be rare but can be quite serious.

Even faced with the threat of an occasionally deadly H1N1 influenza in 2009 and 2010, many Americans refused to be vaccinated. It would be nearly impossible to persuade them to be vaccinated against anthrax or smallpox on the chance that these pathogens would be unleashed by terrorists.

So the countermeasures will sit in warehouses, waiting for an event. Once smallpox or anthrax is released in a vulnerable population, the countermeasures will have to be deployed on a massive scale in a matter of days, even hours. At DHS we knew that this would be a logistical nightmare. After all, we'd lived through the errors and delays as government tried to improvise in the wake of Hurricane Katrina. An incident of biological terrorism would create the same problems, except the victims might be desperately sick, not just hungry and thirsty, and the rescuers would be delayed longer by fears for their own safety.

Imagine a biological attack in which terrorists release a large cloud of anthrax in an urban area without telling anyone. Even with air sampling equipment in place it might take a day or two to confirm the attack. If everyone who'd been exposed took antibiotics within three days, practically all of them could be saved. The weapon could be defused. But if it took five or six days to start antibiotics, we could lose half the population. That's an enormous difference, making every hour of logistical delay a matter of life and death.

So how were we planning to deliver antibiotics? The postal service. That's right. The aggressively unionized postal service workforce would be asked to show up and drive into anthrax-contaminated areas to distribute antibiotics. Of course, they would want armed protection, so law enforcement agents would somehow meet up with the postal workers and they'd both go around delivering antibiotics. To me, this sounded, well, unlikely. Getting the workers to show, hooking them up with their armed escorts, making sure they and their escorts had started antibiotics, verifying the routes, making sure they weren't swamped by people who couldn't stay home for their antibiotics, keeping others from trailing them to steal antibiotics from mailboxes, all of

this would have to be done for the very first time under unbelievable time pressures.

There was a way to cut through this mess. If everyone had their own medical kit of antibiotics at home, all they'd have to do is open it and start taking antibiotics as soon as the attack was discovered. We'd save days of delay and avoid the chaos of distribution. Even if only one-fourth of the exposed population had antibiotics, that would take a load off the distribution system. And in a pinch, people could share their antibiotics, so they wouldn't need government distribution until a week into the course of treatment. That would buy us time and ease the crisis no matter how many people had the home med kits. Not only that, it would leave people in charge of their fate. Instead of being helplessly dependent on government action, they could actively plan for and assist in the emergency.

That's also why the bureaucrats of Health and Human Services hated it. Government officials rarely doubt their own capacity to direct the lives of ordinary citizens. Doctors too seem to have vast confidence in their own judgment, at least as compared to patients. So it shouldn't be a surprise that government doctors have no faith whatsoever in the great unwashed mass of citizens. The Public Health Service has, basically, one piece of advice for the public in any health emergency: sit tight and wait for our instructions. We'll decide who should get vaccines or antibiotics, and in what order. If it's a close question, we'll send you to your family doctor, and he or she will tell you what to do. On no account should you do anything to help yourself. If you try to buy antibiotics, you'll be "hoarding" medicines that are needed more by others, like, uh, medical professionals.

When the first anthrax attacks occurred, that's exactly what government doctors said, and their guidance was posted on government and American Medical Association Web sites. Anyone trying to obtain Cipro or other antibiotics was seen as ignorant or selfish or both. In addition to the fear that medicines wouldn't be rationed in accord with government priorities, medical professionals were understandably concerned about the overuse of antibiotics, which has

encouraged the evolution of antibiotic resistance. So letting ordinary people have antibiotics in their homes was considered too risky. They might take it for a headache.

So the med kit idea met a wall of medical and bureaucratic resistance, even though both the secretary and deputy secretary of Health and Human Services eventually became supporters of the idea. Unable to defy their superiors, the bureaucrats who worked for them slow-rolled the idea. Eager to prove that you and I can't be trusted, and to wait out their bosses, they insisted on a large-scale test, putting emergency kits in the hands of citizens and telling them not to open the kits except in a government-announced emergency. I was delighted when they had to report back to the interagency that only one person had opened the kit improperly—an elderly woman who heard an official tornado emergency announcement and opened her package in the hope that it might offer some guidance.

Since the study hadn't turned out quite the way the bureaucrats expected, it was clear that what we needed was, well, more studies. The leaders of DHS and Health and Human Services pushed hard for a better set of plans to distribute med kits and use other methods to avoid the postal service option. In the month before the election, despite concerns that we'd look as though we were spreading fear, the two departments announced a number of steps that would make med kits possible. But time had run out; the efficacy of med kits was still being studied (in a Minnesota pilot project) when the Bush administration left office.

A year later, the bureaucrats won. An unimaginative bioterror strategy was released by the White House in December 2009.[3] It contains an inevitable section, beloved of bureaucrats, setting out everyone's "Roles and Responsibilities." Such documents are beloved of bureaucrats because that's where all the turf wars are fought.

Now, you and your family probably didn't hire anyone to participate in those turf wars on your behalf.

Believe me, it shows.

Because when the document sets out your roles and your responsibilities (*i.e.*, the roles and responsibilities of "Individuals and Families"), here's what it says:

> There is a critical role for families and individuals in reducing the risks from biological threats. Individual contributions to community resilience can undermine motivations for biological threats by reducing their effectiveness. We will encourage individuals and families to undertake the following:
>
> - Following general guidance for disaster preparedness, such as keeping supplies of food and other materials at home—as recommended by authorities—to support essential needs of the household for several days if necessary;
> - Being prepared to follow public health guidance that may include limiting their mobility throughout the community for several days or weeks, or utilizing designated evacuation routes; and
> - Informing appropriate authorities when they encounter or observe suspicious or unusual activities.[4]

This language was surely meant to resolve the bureaucratic battle conclusively against do-it-yourself preparedness. It says individuals are supposed to "follow guidance" about keeping food and other materials at home. But in case you didn't understand the first time that you're only supposed to do what the government tells you, the bit about keeping materials at home gets an added and quite redundant qualifier. While you're following government guidance about keeping materials at home, remember that you're only to keep materials "as recommended by authorities."

And how will you get, say, antibiotics in an emergency? That shoe dropped a few weeks later. The Obama administration decided to make a big bet on the postal service's nimbleness, sense of urgency, and dedication to duty. In a Christmas week executive order[5], it announced plans to bet your life on the postal service having all those qualities and more.

Stop for a moment to imagine the scene. Postal workers will be asked to drive into contaminated neighborhoods even though they can't be sure their countermeasures will work against whatever strain has been spread there. The neighborhoods will be full of people desperate to get antibiotics, so for protection, the postal workers will first have to meet up with guys with guns whom they've never seen before. They also have to collect antibiotics from pickup points that they may or may not have seen before. They'll meet the guys with guns there, or someplace else that may have to be made up at the last minute. Then they'll start out on routes that almost certainly will be new to them. As they go, they will be expected to seamlessly and fairly make decisions about whether to deliver the antibiotics to homes where no one is present, to rural mailboxes that may or may not be easily rifled, to people on the street who claim to live down the way, to the guys with guns who are riding with them and have friends or family at risk, and to men in big cars who offer cash for anything that falls off the truck.

And this will put antibiotics in the hands of every single exposed person within forty-eight hours, from a no-notice standing start?

No way. It will be a nightmare. And that's not a knock on the postal service, which may, in fact, be as good a public agency as any for getting antibiotics into the hands of an exposed population.

That said, no one but an idiot would bet his life or his children's lives on flawless execution from a public agency doing something it's never done before.

So here's what I did—and what you should do, too. I asked my doctor for an emergency supply of antibiotics that would get me through the first week or so of a crisis. I promised not to take the antibiotics irresponsibly for colds or other viral infections. And I was ready to change doctors over the issue.

I got the prescription.

Some public health officials may try to make you feel guilty about "hoarding" antibiotics or contributing to antibiotic resistance. Poppycock. If you buy while supplies are plentiful, you're actually creating a bigger market for these products and contributing to the maintenance

of production capability. And if you don't take them in response to a tornado warning, you won't affect resistance.

In fact, you're being socially responsible. If we do suffer an anthrax attack and the postal service has trouble keeping up, a sure bet if ever there was one, you can defer your delivery in favor of someone who has no stash. You'll take a bit of strain off a system that is going to need all the relief it can get.

And for those who'd like to recapture their youth, in addition to the glow of virtue, you might even feel a bit of leftover sixties civil disobedience thrill. When I tried to give this home stockpile advice in a speech toward the tail end of the last administration, the lawyers at Health and Human Services told our lawyers that I'd be violating the law—because advocating an unapproved use of prescription medicine is a criminal offense under the federal food and drug laws. And, while taking antibiotics for an anthrax attack is an approved use, getting antibiotics in case of an anthrax attack is not. If the Health and Human Services lawyers were right, then this part of the book would be a felony. I think they're full of it, or I wouldn't be writing this. But if I'm wrong, well, power to the people.

The new policy is a throwback to an era of government-knows-best. There's a big role for government in countering terrorism, but this isn't it. This is like telling passengers that the best response to an air hijacking is to sit tight and wait for the authorities to arrive.

It's insufferably paternalistic. And it's bad advice.

So the bad news is that the administration isn't going to help you prepare a home med kit. No standard packaging and labels, no encouragement for doctors to prescribe the kits responsibly, no sober discussion of the risks. You're officially discouraged from worrying your sweet head about such things.

The good news is, no one will listen.

At least, not if I can help it. In fact, since no one in government has followed through on the claim that my advocacy of home med kits is illegal, you've got an easy response if government doctors try to discourage you from getting a home stash. Just tell them you're

adhering to the roles and responsibilities in the administration's bioterrorism strategy: You're keeping material at home "as recommended by authorities"—two of them, the authority of this book and of your own common sense as an independent citizen.

The other government program to thwart biological terrorism is based on the Willie Sutton principle. Sutton robbed banks "because that's where the money is." If you want to prevent the release of pathogens, probably the best place to start is where they are. And the people who ought to get the earliest scrutiny are those who have regular access to those pathogens. Because history tells us that bugs in the lab have a way of ending up in the wild.

In February 1978, Christmas break was a distant memory for the cadets of the U.S. Air Force Academy near Colorado Springs, Colorado. They were grinding their way through the bleakest stretch of the academic year. Suddenly, in less than three hours, five hundred of them had lined up outside the academy's clinic. They had the flu, and within days, three-fourths of the student body had fever, sore throats, headaches, and weakness.

Yet the faculty suffered no ill effects. They lectured to nearly empty rooms. Later, researchers pieced together the flu's origins. It was an H1N1 virus, very like one that had circulated in 1950. That explained why the cadets fell ill while the faculty did not. The older instructors had already been exposed. The younger ones had not. Still, the older faculty's resistance seemed surprisingly complete.

The reason for that soon became clear. The virus that hit the academy wasn't just similar to the 1950 version. It was identical. Now, nature doesn't usually repeat herself so precisely. But human researchers do. Many scientists think the 1977-78 influenza was released from a store of the 1950 strain—in error or otherwise. We still don't know.

Twenty-three years later, though, there wasn't much doubt that someone could release a pathogen from an existing store. According to the FBI, Bruce Ivins exploited his status as a biodefense worker at Fort Detrick in Maryland to obtain enough anthrax to kill seven people.

Fears of an inside job led Congress to adopt the "select agent" program in 2002. Its purpose was to keep the worst pathogens out of the wrong hands. It called on the Department of Health and Human Services to identify truly dangerous pathogens such as Ebola, plague, and anthrax. Researchers who wanted to work with these agents had to register their facilities, name an officer who was responsible for security, and prepare both a security and a safety plan for the agents. Those who worked with the agents had to undergo background checks; they were to be listed in a database and checked against criminal and immigration records. Foreigners who passed a background check could work with the agents if they did not come from a country that sponsors terrorism. All shipments and handling of these materials had to be tracked, and exports were subject to control.

DHS didn't exist when the select agent program was created. But we thought we had something to offer. The program was trying to solve a problem that looked a lot like the problem we faced at the border. Most lab workers, like most travelers, are entirely innocent; we want them to keep doing exactly what they're doing. So we needed a way to separate the great mass of ordinary researchers from a few risky ones. In the travel arena, the key was good data about travelers. If we knew who was coming to the United States, and we had a good idea who was risky, we could concentrate our attention on the tiny minority of risky travelers.

The same was true of researchers. In fact, that was the theory behind the select agent rules already enacted. Anyone with access to highly dangerous pathogens would be identified and investigated by the FBI. If the bureau had reason to think the researcher was a risk, access to the pathogens could be denied. But the FBI is at heart a criminal investigative enterprise. It doesn't make the kind of screening decisions DHS has to make every day at the border.

So DHS maintained electronic databases that offered up-to-date information about who was coming to the United States and who was a security concern. The select agent records, in contrast, were kept in paper files, or at best were frozen electronic pictures of documents

rather than easily searched electronic data. This meant that the FBI performed a one-time check on each researcher, using this paper record. Once that person was cleared, there was no good way to go back and look at his or her record without doing a paper search. As a result, the records simply sat in file cabinets for years. If a new fact showed up that made a researcher seem more risky—calls to a known terrorist, for example, or a decision to overstay his visa illegally—the federal government might never know that he also had access to an extraordinarily dangerous biological agent, at least not without getting out the paper files and checking names.

That didn't seem sufficient to us; we thought that researchers with access to the most deadly biological agents on the planet should get at least as much scrutiny as sleepy tourists arriving from Munich or Bangkok. We offered to put the files into a modern database or spreadsheet format so that they could be cross-checked automatically on a regular basis. We knew that even this would not be a foolproof system. A well-organized terrorist group could recruit people with clean records to work at pathogen research facilities. But it's almost always a mistake not to do something about terrorism risks just because you don't have a 100 percent guarantee of success. Terrorists are human, too. Sometimes they can be discouraged by measures that might not hold up to extended testing. And sometimes their efforts to evade and test your systems will backfire, drawing attention to the plot. The more information you have, the more likely you are to spot these efforts.

Since our approach to the problem of biotechnology involved learning more about researchers, we could expect privacy objections. But all we were proposing was to digitize records that had already been given to the government for purposes of background checks. You wouldn't think that privacy groups would object to government doing a better job with data it already had. At least that's what DHS thought. But in the end we didn't get a chance to find out how they'd react.

DHS was the new boy. The FBI and Health and Human Services had been given responsibility for the select agent program by

Congress before DHS was even created. They didn't get along particularly well, but they agreed on this much: They didn't need a third agency involved in the program, no matter what improvements the agency was willing to pay for. When we asked HHS which research labs held select agents, something we'd have to know to perform any review—or to plan a rescue if a flood, hurricane or earthquake struck the laboratory—HHS staff simply refused to provide the data. Even after the secretary of HHS twice promised our secretary that the data would be sent, his staff refused.

To justify their stonewalling, both the FBI and HHS played the privacy card. They told us they couldn't give DHS access to the background check data because, conveniently, they hadn't mentioned such information sharing when they wrote the privacy statement explaining how the data would be used. They'd have to publish a new privacy statement, then take comments on the change, then respond to the comments, they said, and maybe, maybe then, they could give us access.

We'd been down that road before. Even routine changes to a privacy statement take a year-and-a-half. And that's assuming the agency wants to make the change. If the agency didn't want to do it, the opportunities for delays and detours were endless. The FBI began the process, but I wasn't surprised that it hadn't been completed by the time we left office.

Maybe it never will be. One of the open secrets of the federal government is that privacy concerns can often be a useful way to advance bureaucratic interests without sounding parochial. ("We're not turfy; we're civil libertarians.") No agency likes to share information with another. The other agency may use the information successfully but not share credit. Or it may use the information to second-guess the operations of the agency that gathered it. That's one reason the wall was so difficult to eradicate. Privacy claims simply reinforced a natural bureaucratic instinct to hold information close. In 2001, that mix of turf and privacy constraints had cost us dearly. For a while, it had receded as we counted the cost. But this was a different threat, and as we turned the reins over to a new administration, all the old instincts had revived.

And just like the fight over the wall in 2001, privacy groups had won this fight without even having to show up. The rest of us had lost.

That was frustrating; it was also just the beginning of our difficulties. The select agent program was based on an assumption that wouldn't be true much longer. Congress had assumed that we knew where the pathogens were. It hadn't prepared for a world where pathogens could be assembled from the blueprints of life.

History had already demonstrated that even the workers in government labs couldn't be fully trusted to keep pathogens under lock and key. What were we going to do when anyone with access to the DNA sequence of a pathogen could simply build it—or, even more simply, order it from a foundry?

We probably had a few years to find a way to head off this nightmare, but we needed a plan. I began to consult biotech experts, looking for someone who understood the technology, the risks, and perhaps some of the opportunities.

Craig Venter is a bald man with a beard and the tanned, bulky fitness of a sixty-year-old defying his years. He leans across the DHS conference room table as though he owns it. But the meeting isn't going quite as smoothly as Venter expected.

Venter is used to government meetings. He'd been a government researcher himself, long ago. But now he is a kind of biotech rock star, famous for sequencing the human genome in a bitter, elbow-throwing race between the National Institutes for Health and an upstart private company he created. Venter's company caught the NIH from behind, and the drama of the chase helped Venter raise a billion dollars for his company.

Venter learned then that sizzle sells, and he's a master at creating a narrative that catches journalists' imagination. In a second biotech undertaking, he sailed around the world, dipping into the ocean and parsing the DNA he found there. Now he's launched on his third—a private effort jump-started with government funds that has already

assembled nearly 600,000 base pairs to make the chromosome of a bacterium. He hopes to create an artificial organism that will make hydrogen or ethanol for industrial fuels.

If anyone represents the promise of biotech, it is Venter. He sees engineered organisms as the key to progress and riches on a vast scale. So he can't be comfortable with the theme of the meeting.

I am pressing him on risks, not promise. Venter knows more about biotech than almost anyone. If there's a way to avoid the dangers that come with democratizing genetic engineering, Venter should have it at his fingertips.

"What will stop terrorists from inventing new diseases?" I ask. Even if they're afraid of blowback that infects their supporters, plenty of pathogens affect different ethnic groups differently; and some viruses cause genetic mutations. Won't we see groups or individuals trying to engage in a kind of DIY eugenics—improving the species by killing off disfavored racial or ethnic groups or by introducing new genetic material to make future generations more peaceful and compliant?

They wouldn't even have to succeed to cause a disaster, it seems to me. A badly coded biological virus probably won't act like a badly coded computer virus. Bad computer code usually does more or less nothing. The computer's default state is inactivity. But in the biological world, the easiest way to build a new organism is to start with one that already exists and then change a few genes. That means using one that's been honed by billions of years of evolution to survive—to feed and breed at all costs. Even if the new gene turns out to be defective, the resulting organism could find a way to keep on feeding and breeding. We don't know what it will feed on or how quickly it will breed, but any surprises on this front are likely to be bad ones.

I'm thinking of what happened in 2001, when an Australian research project went frighteningly wrong. The researchers were trying to create a rodent contraceptive from the mousepox virus. They spliced a gene into the mousepox virus. They didn't want to hurt the mice, so they injected the engineered virus only into mice bred for resistance to mousepox. And, adding suspenders to

their belt, they vaccinated some of the mice for mousepox before administering the injection.

As a contraceptive, it turned out, the new virus was an overachiever. Dead mice don't have sex, and dead mice were what the virus produced. The new gene turned the formerly mild mousepox virus into a killer, overriding the genetic resistance of every unvaccinated mouse. And then it turned on the vaccinated mice, killing half of *them* for good measure. If just one researcher made just one mistake as bad as that with human subjects, I tell Venter, even nations that had stockpiled vaccines would be destroyed. How do we know, I say, that well-intentioned hobbyists, not to mention hapless terrorists, won't produce pathogens that are far more lethal and contagious than they intended?

Truth be told, this is turning into a bit of a rant, but I'm still not done. I'm not going to have another chance to get biotech advice from a rock star. Perhaps mistakes and terrorism aren't even the worst we have to fear, I offer. Computer viruses became ubiquitous only when hackers realized that they could make money from the infections. They had invented a new form of organized crime. Why couldn't the same thing happen in biotech? If we don't know who has released a pathogen, couldn't some crooked business, somewhere in the world, be tempted to design a disease, patent a cure, and then let the disease loose upon the world? Even if others suspected wrongdoing, the sick would still pay whatever it costs to get well, and with the proceeds, a company could buy a lot of protection from its government. What can we do to keep foreign businesses from trying such a tactic?

I pause. That's a lot to put on the table. But at least I've laid out all my concerns. I'm hoping Venter can see something I've missed, some reason why democratizing this technology won't ultimately empower the worst in human behavior as well as the best. Or at least some way to keep his beloved technology from putting humanity at risk.

I wait. Venter leans in, clears his throat. He smiles the winning smile that has charmed reporters and government funders for more than a decade.

"My, my, don't *you* have an imagination," he beams.

That's how it goes with many of the biotech leaders I consult. They know what the risks are. They just don't like to talk about them.

Rob Carlson is a principal at Biodesic and one of the industry's most astute observers. A physicist by training, he's spent years studying biotechnology as a business and a human undertaking.

Carlson has close-cropped hair and a genial, wonkish air. He's an eager teacher. But he grows distinctly uncomfortable when I turn the conversation to bioengineered pathogens.

Carlson wants to talk about where the industry is going. Biotech has already produced enormous improvements in productivity, he says. Drugs developed with recombinant DNA already have sales of $65 billion a year, and biotech products already account for 2.5 percent of GDP growth. One company has modified yeast into a bug that can transform sugar into everything from malaria drugs to jet fuel and gasoline. Production will begin in 2010. And many companies expect to build bugs that can produce other chemicals out of petroleum. The chemical industry could be transformed by bioengineering, Carlson argues, but these changes cannot be achieved without making the tools for bioengineering cheaper and more efficient.

So, cheaper they will get. And bioengineers everywhere will benefit. Already, the foundries that assemble small bits of DNA into large stretches have been driven by competition into fully automating the process from code to gene sequence. Even so, the biggest bottleneck in industry is the time engineers spend waiting around for foundries to send back the sequences they've ordered. The engineers don't want to wait. Carlson thinks the chemical industry's need to experiment quickly with many different genes and organisms will continue to force the pace of automation until the process can be performed in a single machine that can be run by the engineers on premises. That machine will grow cheaper and smaller at an exponential rate because of the returns and the integration of semiconductor processes. The result will be desktop DNA synthesis, Carlson predicts, and perhaps very soon.

When that happens, he sees a golden age of bioengineering. Bugs will eat our waste—literally, feasting on municipal sewage—producing

raw materials that other bugs will turn into plastics and chemicals. Energy independence may come to any nation with modern sewers. The opportunities are astonishing.

I interrupt. Yes, I know. Biotech is irresistible. But that desktop DNA synthesizer—who's going to use it besides chemists? What about all the bad things that will come from putting this power into everyone's hands?

Carlson blinks. Well, sure, there could be bad things. Terrible things, maybe. But with technology like this in our hands, we can devise countermeasures faster and make them more effective than we ever dreamed possible. A revolution is coming. Why do you insist on looking at the downside?

He pauses and returns to the emerging economic opportunities. The industry is already global, and the business logic of bioengineering is already established. It's a fantastic new technology that will transform our lives for the better. Surely we'll be able to handle the risks in that transformed world.

After all, I think, who wants to be the voice of doom when everyone else is hoping to be the Steve Jobs and Steve Wozniak of biotech, playfully hacking genomes and starting a global empire in the garage?

Silicon Valley and the computer revolution is exactly what Rob Carlson and the rest of his generation hope to emulate. A growing "DIY bio" movement shows bio-hackers how to extract and modify DNA on their own, using household equipment. There's a *Biotech Hobbyist* magazine with a "series that will show you how to grow your own skin culture and suggest some very cool projects you can do with it."

There's even a biotech version of the Linux open source operating system. "Biobrick" prizes are awarded to teams that create standardized open-source DNA parts that perform predictable biological functions and can be combined in new ways.

Today, colleges hold lighthearted competitions for the best biological design. MIT's winning team in 2006 re-engineered *Escherichia coli*—an organism that lives in the human gut and helps to give our waste its distinctively foul smell. When the students were done, the redesigned E. coli smelled like wintergreen.

Biotech: it's cute, it's fun; and then you get rich.

I remember when the computer software geeks first came to Washington in the early 1990s. They were shocked to hear that the government wouldn't let them offer strong encryption to the world. The government feared that unbreakable encryption would allow criminals, terrorists, and pedophiles to hide evidence and communicate without fear of wiretaps. The technologists dismissed the fears. Encryption would be necessary to do business on the Internet, a development that was inevitable, they said, sounding a lot like Rob Carlson. Government would just have to get out of their way.

Carlson and other biotech industry representatives have none of the software industry's in-your-face contempt for government. After all, many of them are funded by NIH and hope to develop treatments that will pass muster with the Food and Drug Administration. Instead of defiance, they offer deflection, simply gliding past the risks and averting their gaze. It's the way most of us deal with the animal experiments that make new drugs possible: They're unfortunate, tragic even, but that's the price of progress; now, can we talk about something else, please?

Sixty-five years ago, with a bright flash and a mushroom cloud, the nuclear age was born in the New Mexico desert. Robert Oppenheimer was a prime mover in the first nuclear test, and he later told how the scientists reacted:

> We knew the world would not be the same. A few people laughed. A few people cried. Most people were silent. I remembered the line from the Hindu scripture, the *Bhagavad Gita*. Vishnu is trying to persuade the prince that he should do his duty and to impress him takes on his multi-armed form, and says, "Now I am become death, the destroyer of worlds." I suppose we all thought that, one way or another.[6]

Nuclear technology came into the world burdened by a sense of original sin. Before it became a source of cheap, carbon-free energy, it would kill and wound two hundred thousand people in Hiroshima

and Nagasaki. For nuclear scientists even their most satisfying work was alloyed with tragedy.

It's a long way from that sober sense of guilt to the spirit that gave the world E. coli that smells like wintergreen. That's because, with nuclear technology, the deaths came first. With biotech, as with jet travel and computer networks, it's the delight, and the profits, that have come first.

It's odd. No one in the industry denies the risks, and some can be eloquent about the need to address the problem. But a curious disconnect remains between their intellectual acceptance of the danger and their response to it. At a visceral level, many of the biological and medical researchers who are leading the revolution simply cannot believe their technology may end up causing more harm than good. Some of them seem convinced that doctors, or at least medical researchers, just aren't the kind of people who would do such a thing. And so they fight restrictions on their work with the fervor of men and women who are determined to make the world a better place—no matter what the bureaucrats say.

DHS had no authority to force the foundries to screen their orders. Many of them were overseas, and none were subject to direct regulation. But we decided to press them anyway. We might not have regulatory authority, but we could make noncompliant foundries uncomfortable. We met with some of the DNA synthesis companies and told them they had a responsibility to prevent misuse of their products. They should know each customer and whether the customer was a legitimate business. And they should make sure the string of code they were building was not dangerous—the string of code that gives a pathogen its virulence, say, or the insertion of a toxin into the gene for an edible plant. If they got a suspicious order, they should report it to the government.

The purpose of this screening wasn't just to keep terrorists from building pathogens. We were also thinking about attribution after an attack. If we are attacked with an agent that might have been engineered, we will quickly find the resources to review

every synthetic DNA order in recent years—and to interview every purchaser whose orders resemble the pathogen. But if the foundry doesn't keep records, we can't review them later. Quickly identifying the attacker is one of the great challenges of biological terrorism; if we can do that, we will deter many future acts and we will reassure our citizens that their government is not helpless in the face of what could be a devastating attack.

Measured against the horrors and risks that come with exponential biotechnology, that may not seem like much of a response. But it was a start; it reflected a core strategy of expanding the information needed to identify risky people, either before or after an event. And if it seems like too little too late to you (as it does to me), there were plenty of officials who were prepared to fight even these modest steps.

Some of the American and European foundries were responsive. A few had already begun screening customers and keeping records. They were in business for the long haul, and they couldn't afford to acquire a reputation for irresponsibility. That was worth something, but if other foundries refused to screen orders, then we'd just be moving the risky customers to the irresponsible suppliers.

DHS's proposal to press the foundries to engage in screening met with a tepid reaction at the lower levels of HHS. The NIH, in particular, was so sure that basic research in biology was a boon to mankind that it refused even to keep track of who was accessing the research on dangerous pathogens that it published on the Internet. Researchers who blithely published work that could be used both for weapons development and energy production would be widely condemned as dangerously irresponsible; but unrestricted publication of biological research is still an article of faith, even though such research can also be used both for commercial and military purposes.

Only after members of the industry and two independent biosecurity boards had made similar recommendations did NIH agree in principle to do something about foundry screening. NIH proposed to tell its grantees that they should send orders only to foundries that engaged in screening.

For other countries, controlling biotechnology was simply not on the agenda. Biotech expertise had spread throughout the world. Nations that missed the information technology boom were rushing to stake a claim in the next hot field. Commercial DNA foundries can be found in California, New York, and Massachusetts, of course, but also in Pretoria, Moscow, Dalian, and Tehran. Where we saw a global risk requiring oversight, these capitals saw a chance to catch and pass the United States in the exploitation of biotechnology. They still chafed at the role that Intel and Microsoft played in information technology. Why couldn't the Microsoft of biotech be Chinese or Singaporean or Dutch, they asked? If the United States wanted to hobble its researchers with elaborate restrictions, well, fine. That was an opportunity not to cooperate with the United States but to steal a march on it.

If pressed for cooperation, international diplomats argue that the key is enforcing the Biological Weapons Convention. This is an example of just how wedded to the status quo international diplomacy can be. The Biological Weapons Convention is modeled on treaties to control nuclear weapons that can trace their roots back to the 1940s, when U.S. policymakers hoped to move from nuclear weapons to the peaceful production of nuclear power. The nuclear weapons convention adopted in the 1970s seeks to follow the same pattern; it offers a simple bargain to countries that lack nuclear weapons: Abandon military use of nuclear technology and the countries that have weapons will teach you how to use nuclear technology for peaceful purposes. Every five years, the nuclear haves and have-nots get together in Geneva. There, the have-nots press the haves to abandon nuclear weapons before they get down to the less high-minded task of demanding more aid and more technical assistance in using nuclear technology.

The Biological Weapons Convention more or less borrowed the same model when it was adopted in the 1970s, even though it was never a good fit. The nuclear convention makes at least some sense because there is a vast difference between building a nuclear power plant and building a nuclear weapon. Information about the peaceful

uses of nuclear technology is not easily used in a weapons program. So it's possible to transfer peaceful-use technology without dramatically increasing the risk of weapons proliferation.

That's not true for biological technology. There's no real difference between a bioengineering facility meant to cure disease and one meant to cause it. Facilities can be switched from one purpose to another with little more than a long weekend and a few gallons of bleach. Inspections to catch cheaters would have to be deeply intrusive, could easily become a cover for the theft of intellectual property, and would almost certainly fail to catch countries that were serious about maintaining an illicit program. The advent of synthetic DNA, with its radical empowerment of all researchers, makes the model even less relevant.

If ever there were a doubt about the dysfunctional conservatism of international forums, the persistence of the Biological Weapons Convention surely should put an end to it. The risks of biotech are novel and pressing. But the solution posed by internationalists is to draw on a model that was adopted for nuclear weapons in the 1970s and hasn't been a notable success in the forty years since. Finding a new response to a new problem seems to be simply beyond the capability of the international community.

In short, we were on our own. DHS kept pressing for action on foundry screening. A year after we left office, five of the biggest DNA foundries agreed on a common screening protocol that they would apply to every synthetic gene order; they also agreed to keep customer records for eight years.

This was progress, if it actually survived scrutiny by the European privacy bureaucracy. (European members of the group did not explain how they would square this new practice with the EU requirement that order data be destroyed when no longer needed for commercial purposes.) But at best, it covered only 80 percent of the foundries by market share.

Domestically, in 2009, HHS issued voluntary guidelines meant to encourage and set standards for screening of foundry orders. But

the incentives to follow the guidelines remained limited. Exponential growth in the market has made NIH's standards less important. Today, NIH grantees probably account for no more than 10 percent of the foundries' business. Foundries that find the standards constraining can simply limit their sales to customers who aren't using NIH money. And if the United States tries to make the rules mandatory, they can take their facility elsewhere; biotech firms are likely to be welcomed in other countries with open arms and less demanding laws.

In a globalized world, where regulations may be put on the block to get an edge in the international competition for new industry, is there any way to prevent a race to the bottom on synthetic DNA? Perhaps, but only over the opposition of privacy, business, and other governments. If the United States really wants to ensure that biotechnology researchers and developers meet biosafety and biosecurity standards, it can use the one piece of government leverage that still counts in that world.

For biotech firms, the road to riches is intellectual property. A patent entitling firms to a royalty on the exploitation of some new biotech technique or drug is the key to most startups' business plans. And U.S. patents are particularly important because, in the absence of government medical price controls, the U.S. market probably pays a disproportionate share of the development costs for new drugs.

If all companies seeking patents derived from biotech research were required to demonstrate compliance with reasonable safety and security measures, the requirements would likely be observed globally, since even companies located in deeply hostile nations, such as Cuba, have sought U.S. patents for their research. (Despite sanctions and a bitter war of words between the two countries, Cuba has been granted more than seventy-five U.S. patents in the last thirty-five years.)

Of course, the governments that would be bypassed by such a measure can be counted on to protest, as will the business interests

that want intellectual property protection without regard to their security record. And, since the most obvious biosecurity measures include detailed records of who is performing what kinds of research, we can expect other nations and the business community to cloak their interests in a cloud of privacy objections.

Requiring biotech companies to demonstrate that they have met biosecurity standards in order to get patent protection might well work, but it's guaranteed to trigger hostility from business, privacy, and international interests, and that's why it probably won't happen, at least not until the ever-steepening curve of biotechnology produces a disaster.

The Hoover Institution on War, Revolution and Peace, founded at Stanford University in 1919 by Herbert Hoover, who went on to become the thirty-first president of the United States, is an interdisciplinary research center for advanced study on domestic and international affairs. The views expressed in its publications are entirely those of the authors and do not necessarily reflect the views of the staff, officers, or Board of Overseers of the Hoover Institution.

www.hoover.org

Hoover Institution Press Publication No. 591

Hoover Institution at Leland Stanford Junior University,
Stanford, California, 94305–6010

First printing 2010
16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

Manufactured in the United States of America

The paper used in this publication meets the minimum Requirements of the American National Standard for Information Sciences—Permanence of Paper for Printed Library Materials, ANSI/NISO Z39.48-1992. ♾

Cataloging-in-Publication Data is available from the Library of Congress.
ISBN-13: 978-0-8179-1154-6 (cloth)

ISBN-13: 978-0-8179-1156-0 (e-book)