Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science
Volume 7, Number 4, 2009 © Mary Ann Liebert, Inc.
DOI: 10.1089/bsp.2009.1201

Profile

Gerald L. Epstein, PhD

Director, Center for Science, Technology, and Security Policy, American Association for the Advancement of Science (AAAS)

Over his entire career, Gerald Epstein has toiled at the nexus of science, technology, and security. From 2003 to 2009, he was Senior Fellow for Science and Security at the Center for Strategic and International Studies Homeland Security Program, where he worked on reducing biological weapons threats, improving national preparedness, and easing potential tensions between the scientific research and national security communities. Epstein came to CSIS from the Institute for Defense Analyses. From 1996 to 2001, he served in the White House Office of Science and Technology Policy. And from 1983 to 1989, and again from 1991 until its demise in 1995, Epstein worked at the Congressional Office of Technology Assessment, where he directed a study on the proliferation of weapons of mass destruction, alongside research on other global security topics.

A recognized expert in biological risk reduction, Epstein was actually trained as a physicist, having received SB degrees in physics and electrical engineering from MIT, and a PhD in physics from the University of California at Berkeley.

How, then, did he come to study the evolving threat from bioterrorism? "What compelled me about bioterrorism was that it was a stellar example of a topic that would lead to a train wreck between the scientific community and the security community unless they figured out how to work together," he said. "The distance between a laboratory and a very large consequence event is a lot shorter in biology than in any other field. I got into bioterrorism to help make sure that the security community doesn't get so scared of the science that it shuts it down, and that the science community isn't so oblivious of security concerns that it pays no attention to them."

Epstein spoke on November 6, 2009, with contributing writer Madeline Drexler, author of *Emerging Epidemics: The Menace of New Infections* (Penguin, 2009), an updated version of an earlier volume. Drexler holds a visiting appointment at the Harvard School of Public Health and is a senior fellow at Brandeis University's Schuster Institute for Investigative Journalism.

Q: In 1993, you directed a study at the Congressional Office of Technology Assessment that became a classic in the biosecurity world. You estimated that 100 kilograms of aerosolized anthrax, released over Washington, DC, would kill 130,000 to 3 million people. Do you still hold by those numbers?

A: That estimate involved a lot of assumptions about dispersing very high quality, very aerosolizable anthrax, and the high end represented conditions that were extremely favorable to the attacker. Given all the uncertainties, those numbers are reasonable, assuming the attack worked at all. Considering the ways that an attacker can screw up, though, the estimate should probably have gone down to zero. One criticism we got was that there weren't 3 million people in Washington, DC, to kill. But there are more than that many people in the metropolitan area—

and if we were off by a factor of a few, that doesn't change the bottom line. It was meant to illustrate what the maximum theoretical possibility could be—a way of saying, "This could be a very serious threat to national security." However, it's not necessarily something we have to wake up every morning and worry about.

Q: Are the study's assumptions still realistic?

A: It was 100 kilograms of very high quality anthrax delivered by an airplane going across the wind. We had a nation-state in mind; we didn't assume that a terrorist group would aim at making that much or that it would succeed at doing so without getting caught. The point was to illustrate what an amount of anthrax that was easily within the capability of a nation-state to produce could do. So it was a very robust attack. You have to work down from there and say, "How many of these things are really likely assuming some particular attacker?" That debate is still going on.

Some people argue that a substate group could conduct a national security scale attack like this fairly readily—maybe not in a single release, but in a number of releases of material over a period of time.

But other people argue that no nonstate group could ever commit an attack on a scale that would inflict a national security wound like that. They say, "There are a lot of other things you need besides getting the bug and getting a fermenter and an aerosolizer. You have to have an organization, social cohesion among the people doing it, motivation. You have to overlay nontechnical factors on top of the technical ones."

It's true that nontechnical factors matter, but I think it's dangerous to assume that they would reliably prevent a large-scale attack. Once you look at the ability of people to use biology to do harm, there aren't many things in the process that are uniquely the province of national governments. I'm not saying it's easy. I'm saying that a dedicated group with enough money and enough time and the willingness to solve problems and overcome obstacles cannot be excluded from causing, if not 1-3 million deaths, then certainly a high fatality rate.

Q: You've written, "Terrorists becoming biologists is less of a concern than biologists becoming terrorists."

A: The idea that people with malicious intent would have a hard time figuring out how to work with an unfamiliar technology would be of some comfort—if that were the case. But if you turn it around, there are lots of people around the world who already know the biology. Very few of them are terrorists—but how sure can we be that no such person would *ever* turn their skills to a dangerous purpose?

This is a global business. These technologies and skills are available all around the world. Even if I trusted every United States researcher, there are a lot of other people around the rest of the world who know biotechnology and about whom I might not be so confident.

Q: You've also noted that not many of today's terrorists have studied biology—but that tomorrow's high school or college biology classes would provide all the education they need.

A: Not necessarily all they need, but the point is that the skills are widely and increasingly available, and people can figure out how to do the things they can't do initially. This is an area that has incredible applications in health, the economy, food and agriculture, the environment, and quality of life. There are more people around the world who are going to know biological things—just like in the 1950s and '60s, when kids all over were playing with crystal radios and electronics kits. Biology is getting there. The next wave of innovation may well be life-based and biology-based, instead of electronics- and physics-based. We're going to have a lot more people who are comfortable with biology. And some of them might find other things to do with those skills.

Q: Could you paint a scenario of a group that may pose a bioterror threat?

A: I don't like getting too specific on things I worry about. But one can imagine a number of ways that groups might pose a problem—including the one that's probably at the top of most counterterrorism communities' list: a group like Al Qaeda—which was known to be targeting the United States, having eminently proven that. It killed thousands of people and had the intention, had one tower toppled on the other, of killing far more. Its statements and publications have aspired to far higher fatality rates than we've yet seen. And we know, based on information that's been recovered in Afghanistan, that it was interested in biological weapons.

Science magazine published a fair amount of information on how far they had actually gotten. It wasn't terribly far. I mean, some of the materials found were crude notes scribbled from a 1950s-era book. The Robb-Silberman commission on weapons of mass destruction intelligence talked about their interest in Agent X. Some say that Agent X was probably anthrax. I don't know if that's ever been confirmed.

But being comforted by the fact that they weren't very far along reminds me of the joke about a man walking in a park who sees a guy playing chess with his dog. He says, "You're playing chess with a dog? I can't believe it! How can a dog play chess?" And the other guy says, "Oh, it's not so impressive. I beat him 2 games out of 3." The point is not that the dog loses most of the time—the point is that the dog is playing *chess.* What concerns me is that a group with this

intention has shown interest in biological weapons. The fact that they were not very far along doesn't fill me with confidence.

The case that's often mentioned as a precedent is the Unabomber. A very technically capable person, living off in the woods somewhere, making handcrafted bombs out of wood, and killing people who he thought were a problem with his view of the world. Compared to things like nuclear weapons and other ways of inflicting harm, biotechnology is more approachable by smaller groups—maybe even down to the level of individuals. People can do things on their own in biology that would be harder to do on their own in other areas. A disgruntled but highly capable person could be a serious concern. For one thing, it's a lot easier to hide the activity of 1 person than the activity of a group.

What I'm not as worried about is a nation-state. A biological weapon doesn't provide much of an advantage for a country. The military in the United States figured these weren't terribly useful, which is why President Nixon was able to get rid of them. It's hard to attack a given site and say, "That hill is now mine, it's not the enemy's." It's hard to control biological weapons, hard to have them be predictable. There are a lot of things about using bugs as weapons that make them hard to model and difficult to use as reliable weapons.

There is also an international ban against biological weapons, which appears to be pretty robust. You do not see countries bragging about having biological weapons. It's like bragging about being a war criminal. Personally, I don't think that many countries have much interest in them. It doesn't mean I give them all a free pass and say we don't care whether you have biological weapons or not. We still should be investing effort in finding out whether they do and making sure they don't.

Q: You mentioned the threat posed by disgruntled scientists. Do you think that Bruce Ivins was the anthrax mailer?

A: I have no way to know that. He could have been, because it's clear that the agent came from a flask in his laboratory, directly or indirectly. There's no scientific question about that.

The question we all have is: How many other people had access either to the flask or to samples that had been taken from the flask at some earlier point? And did the FBI do a good enough job of running down every possible person who could have ever had access and run down every possible sample that came from it? That's a police question. I have no idea.

But the wrong lesson is to conclude that because Ivins worked at Fort Detrick—an advanced high-tech U.S. laboratory with decades of experience with biological warfare agents—that the only people capable of committing an attack like that are ones who work in biodefense labs. Bruce Ivins did have access to a flask of very virulent anthrax, but the equipment he had access to was not that special—it was equipment that other labs in other parts of the world could have readily had as well. So, if it were Bruce Ivins, it's not that he was using special magic wands that only the U.S. national security community possessed. The lesson would have been that Bruce Ivins, having access to that flask and using standard lab equipment, was able to do that.

Q: How refined were those anthrax spores?

A: My understanding is that they were not specially treated in the way that the U.S. weapons program prepared anthrax for weapons use in the 1950s and '60s. It was grown, it was dried, but it was not specially prepared.

Q: If Ivins had not committed suicide, and if you could talk to him today, what would you ask him?

A: "Did you do it?" Presumably, he would say no. But over the course of the trial, with the investigations and the questioning, I would hope that it would have become clear whether he did it or not. I think people ought to have an answer to that.

He was certainly acting bizarrely at the end. And there are lots of questions about whether the Army did see or should have been able to see that he was mentally unbalanced, if indeed he was. However, his deteriorating mental condition as described in the press was manifested at the time he was being investigated by the FBI—it was not his condition in 2001, when the act was done.

So if Ivins was the culprit, the point is not how weird was he acting in 2007 or 2008, but how weird was he acting in 2001. First of all, he may not have been acting in a noticeably strange way then at all. And second, even if he was, it was a different time. If he was acting in ways that seemed a little odd, there may not have been any reason why people would particularly notice or do anything about it, because some of the characteristics that would be defined as a little odd could also characterize brilliant creativity and individual skills in scientific research. So who's to say?

Maybe something that didn't raise a red flag then might raise a red flag now. Was there anything that anybody should have noticed? That's relevant to what we should do to protect ourselves in the future.

Q: In that regard, you've proposed more self-governance in scientific research: having scientists monitor themselves and each other.

A: I hold that out as a question; I don't hold that out as an answer. Can we come up with a way for scientists to be more responsible for each others' activities in ways that won't make them feel like they live in a police

state? I don't think this is a problem that the law enforcement and intelligence communities can solve by what I call "remote sensing"—peering into a lab, peering into a firm, peering into some high-tech enterprise from afar. The best set of sensors to detect illicit activity are the people who are actually working in the same environment. They may be the first ones to know if somebody is acting in a way that may be a problem.

Is there a way to come up with a system that allows us to be sensitive to odd and potentially dangerous behavior in ways that would let us find out about it before it actually results in a serious problem? I don't know the answer.

Q: It seems to be a question, not of technology, but of human intuition, human sensitivity.

A: That's a lot of it. In some sense, it's a cultural shift in the field. Because science is, in many ways, a very individualistic enterprise. We allow people with brilliant ideas and who have skills and incentive to proceed, and we try not to put a lot of barriers in their way. We don't want creativity to be fettered. We want these people to make breakthroughs.

But if that means, "I do my stuff and you have no business asking me about it," that may not be what we need in the future. We need to move toward an era where all researchers and all technologists have some sense of responsibility for the field as a whole. Individuals and small groups have the potential to have a very consequential effect. In that environment, we all have to have a more collegial, social sense of what we are collectively doing.

Q: How does your proposal go over with scientists?

A: If you pose the view that the law enforcement community needs a better look at you guys because you all are potentially dangerous people, that will deservedly get a negative response. But even when you get a little more sophisticated and say, "We're not trying to have a police state, we're trying to have some ability to monitor," then people worry: "Gee, what if I'm doing something totally innocent, but it looks like I might be doing something sketchy?" It makes people nervous.

Whatever system gets set up would have to be done with the acceptance of the community that will be implementing it. The only way it's going to work is if you sit down with a bunch of people, all of whom know how powerful this technology is because they all want to harness that power to do good things for the world. You sit down with them and you say, "This is really powerful stuff. We have a problem if anybody hijacks it. We are all responsible in some way for making sure that that doesn't happen. What can we do?"

Q: You've also written that we need unambiguous regulations that can distinguish appropriate research activities from dangerous ones, but that also have the flexibility to "accommodate changing science, changing circumstances, and surprises."

A: By now, I've become pretty skeptical that regulations can distinguish appropriate activities from dangerous ones, or at least distinguish risky science from safe science. We've been looking for a boundary between the two for years, and it isn't getting any easier to find. That said, there might be some things we can do to help make us safer. They might not be regulations but laboratory practices and oversight and education and awareness and, yes, some kind of monitoring. But any such system has to be flexible, and it has to make sense to the people who are subject to it. The scientific community is particularly resistant to what I call LPS: "Let's Pretend" Security. You can't go to a bunch of scientists and say, "Here is something that cannot possibly work, but somebody out there feels better making you do it, so let's just go pretend it makes sense."

Polygraph examinations at Department of Energy laboratories pretty much fell into that category. There is a role perhaps for polygraphs in a crime investigation. But as a screening device, polygraphing 10,000 people and seeing how many of them have backgrounds you don't want—simple statistics of false positives versus false negatives show that you are going to kick out many more innocent people than you are ever going to catch guilty people. It just doesn't make sense technically. Even if it doesn't bother you to use such a sloppy test on jobseekers, it's a huge problem to use it on those who have been working honorably for years. In the first case, being flagged means having one less job option and losing the chance to serve your country; in the latter, it could mean destroying a career. Imposing a system like that after the fact is far more disruptive and counterproductive than building it in from the beginning, even if it doesn't really make sense then either.

When the Department of Energy came to the nuclear weapons laboratories in the late '90s and said, "We're going to start polygraphing you," there was heated resistance. Because this is a community that knew when a measure that was proposed had any semblance of working and when it was just for show. They concluded this was for show.

Q: The Obama administration and Congress are considering regulations on the biosciences community. What would you recommend if you were the bioterror preparedness czar?

A: There may well be certain categories of people I don't want working in laboratories, who are so manifestly deranged or disturbed that they're not capable of operating safely or responsibly. We need to keep those people out of laboratories. But if we're worried about

people who might secretly seek to do harm, I don't think we know how to find them—and it worries me that we might try to look for them before we figure out how.

I'm more interested in seeing if we can come up with some way of identifying people who are acting in strange ways while they're in a lab—not in predicting who might later act dangerously, but in noticing them if and when they do. There may be people in very stressful situations where everybody agrees, "Maybe it's not safe to yourself or to us for you to be in the lab until your personal situation stabilizes, or until you've had some time to grieve, or whatever." We need a nonadversarial means of taking people out of a potentially dangerous situation.

Q: If Bruce Ivins was indeed the anthrax culprit, would that have been the optimal way to deter him?

A: One hopes. I don't know how he was acting in September 2001. It may have been that no matter what kind of system we had in place—the Epstein Ideal Collaborative Social Self-Monitoring System—there may have been nothing for it to see.

But if you are drying anthrax and milling it and your experiment doesn't call for anything like that—somebody could be in a position to say, "Hey what are you doing?" Or at least tell the lab supervisor.

Q: Let's talk about synthetic genomics. You've written that today it's difficult to fashion a virus that could be used as a weapon, but that in 10 years it may be easier to construct such a virus than to acquire it. Is this a big concern of yours?

A: It's a concern, but I don't know if it's a big concern. Fortunately, it's one risk that we can actually do something about. Because if it turns out to be easier to make a virus than to get it—and if the industry is evolving in a way that makes it more efficient for people to buy their DNA from commercial suppliers than to make it themselves—in other words, if all the DNA used in these types of experiments is being made by commercial vendors—then companies have the ability to screen the orders they're filling. They can ask themselves, "Is this a material which makes sense in a research setting or is this two-thirds of Ebola?" And if it is two-thirds of Ebola, there may well be a reason to be using it, but if so, the scientist must say, "I'm working on Ebola virus, and here's my select agent authorization and my HHS grant."

It's a combination of vendors implementing a process like this on their own and government working with them, either to provide guidance and assistance or maybe to provide a legal framework. It may be that industry doesn't want to be accused of letting a bad order go through, so it has incentives to do the screening itself.

Q: Let's talk about preparedness. Our nation's response to the H1N1 flu pandemic hasn't been stellar. We don't have enough vaccine, we used an old method of making the vaccine, some people are afraid to get the shot, there's misinformation everywhere, there have been logistical problems and inequities in distributing the vaccine. What do all these problems portend for a response to a bioterror attack?

A: They show that it's going to be very challenging to respond to a biological attack. A flu pandemic gives us early warning that something is going to go around the world and may come back later in a much bigger way. It gives us lead time we will never have in a bioattack. But on the other hand, I don't know that any biological attack would reach the scale of a flu pandemic.

Q: In 2002 and 2003, public health practitioners grumbled that bioterrorism preparedness was diverting them from their main mission. Was that a legitimate complaint?

A: To some extent, in public health it was. Money was dumped into the field, but it often came with strings such as: You can't hire people with this, all you can do is buy stuff or find a contractor. So even with the added funds, there was additional demand put on the public health sector, and in many ways they didn't have resources they needed. Even when they had money—and there was a lot of money added in various parts of the public health sector; for example, the laboratory structure was beefed up in a major way—there were areas in which the public health sector ended up with more to do and not enough resources to do it.

To the extent that we think bioterrorism is a real problem, it is a new one, it is added to existing public health concerns that have not disappeared. The result is that life is harder now. But so long as concerns about bioterrorism are legitimate, I can't argue that that shouldn't have happened. It may be that, yes, we have to prepare for that as well as for natural disease outbreaks. We are just in an era where we're going to have to do both. One can hope the policymakers recognize that.

Q: You wrote in 2007, "It is difficult to prove how serious the threat from bioterrorism is." Partly that's because we have very few examples to draw on: the anthrax letters in 2001, the Aum Shinrikyo sarin attack in the Tokyo subway in 1995, the Rajneeshee food poisoning incident in Oregon in 1984. Maybe the risk isn't that great?

A: Maybe so. There are few other areas where there's such a gulf between what we've seen in the past and what might happen in the future. In the fortunate absence of much data, those who argue that the risk isn't that great have as much empirical support as those who say otherwise.

Q: Why haven't we had a bioterror attack in the U.S. since 2001?

A: This country has put an awful lot of effort into disrupting the efforts of groups that we know about. Al Qaeda is being pursued all over the world, and life is being made tough for them. We're actively frustrating them. But one of my bigger concerns about bioterrorism is that the group I may be most worried about is the one that I've never heard of before.

Two things make it hard to predict the future based on the past. One is that technologies are changing. Things are getting easier, more available, more geographically disseminated, and more familiar. The technologies of 2020 are going be a lot different from those of 1980.

We're also seeing new trends in terrorism. Groups are no longer limited, as we had once thought, to some maximum level of damage. The story used to be that terrorists ultimately have some political objective. Even though they see killing people as something that furthers their goals, they recognize that if the attack is too heinous or kills too many of the people whose support they seek, or if it just looks too horrific, it's going to be counterproductive.

What 9/11 told me was that if there is a limit like that, it's a lot higher than we ever thought. Al Qaeda didn't want to kill 3,000 people; they wanted to kill 100,000 people. And on top of that, there may be groups that don't have political objectives at all, and whose lethal ambitions may therefore not be tempered by any sense of backlash.

Who knows what is going to motivate the next person who wants to kill a lot of people? It may be a deranged person. Most deranged people, we hope, are not very functional. So if you're at that level of psychopathology that you want to kill huge numbers of people, one can only hope that you have a hard time feeding yourself, much less making weapons of mass destruction.

But let's say that there's a rare combination of malicious intent and technical capability—so rare that only 1 in 100 million people would ever have that particular combination. What that means is that on a planet of 10 billion people, you've got 100 of those folks wandering around.

All this starts to sound like hyperbole and scare mongering. I'm not predicting that any of these things will happen. Why haven't we seen a major attack to date? I'm willing to admit the possibility that it's because there isn't anybody out there trying to commit one. But I don't see any reason why I should believe that that situation will persist with such confidence that the government should stop spending money on it.

Q: What are the risks of minimizing the bioterror threat? You have written that if we get our response wrong just once, it will encourage other groups to try.

A: I think that's true. If we have a significant biological attack, it will be a horrific event. We will have death and illness. We will pay a serious price for it. But what's really going to matter is whether the population thinks that the government did all it reasonably could have to address the problem—not could we have prevented anybody from getting killed. Given this type of attack, did we deal with it as best we could—or did we end up proving that we have no hope of dealing with such an event in the future?

Hurricane Katrina was a terrible thing—a city flooded, people driven out of their homes—but it might have been handled in such a way that we'd be saying, "What a terrible flood, what a terrible loss of property"—instead of, "What a terrible loss of public order and confidence in government." People lost confidence in government's ability to act.

Prevention is something we need to give more attention to, but I don't think there's reason to expect it's going to be perfect. If an attack happens, hopefully we'll respond to it in a way where we don't have any unnecessary deaths, any unnecessary illnesses—where "necessary" means you can't save the lives of people who have gotten an untreatable dose before anyone knew they were infected.

Q: Do we have the elements of that kind of strong response?

A: We have the elements. You need 3 things: You need to know when you've been attacked. You need to have something to do about it—medications or prophylaxes that are ready to be distributed. And you need to get them out to the people who need them.

We're making progress on all those fronts. We have efforts to look for occurrences of sick people, we have networks of environmental detectors—though there's some dispute about whether that's a promising approach or whether we should either make them much more robust or rely on them less. We have programs to develop medications and vaccines. We have programs to get things distributed.

But I don't think we have done enough. Even though we are spending a lot of money on this—people have pointed to how many billions of dollars we're spending on biodefense, with most of those analyses implying it's too much—maybe what's needed is a lot more. But you do have to justify that kind of investment. You have to make a plausible case that it will, A: be useful, and B: be needed. If no matter how much money you put into it, it isn't going to help, then we shouldn't be spending it. And if an attack on that scale is so implausible that anything we invest in

preparedness is a waste of money, then we shouldn't be doing it.

Those are going to be hard calls—because, again, we're back to estimating the threat. We want to make sure our threat assessments are realistic. But whenever you're dealing with worst case consequences, you're already dealing with things that are likely to be rare. So the question is: How rare? How unlikely?

Yes, we're spending a lot on biodefense, by some measures. But when compared to the United States defense budget, it's actually not very much money. We're spending billions of dollars a year at most on biodefense, and the U.S. defense budget is a major fraction of a trillion—hundreds of billions of dollars a year. If you thought that biothreats were a serious national-scale possibility, would you really want to be spending only a few percent of your total defense budget on them?

Q: Why not put most of the money into public health preparedness?

A: Public health is important; preparedness is necessary to save lives in the event of a biological attack. But it isn't sufficient. We will need to do some things in the event of an attack—like figure out who committed it and stop them from doing it again—that are not relevant to a natural epidemic. Moreover, biosecurity is more than public health. Public health doesn't take into account that people and society feel quite different about a deliberate adversary—one that is not just trying to kill people but to attack people's faith in government and our ability as a nation to exercise independent action. Public health means defending against an unthinking, unwitting adversary. We know that microbes change and evolve and exploit new niches and defeat drugs—but they don't read the paper. And they aren't trying to accomplish a political objective.

Q: You have written that a bioattack is a law enforcement issue, a counterterrorism issue, a national security issue, a disaster management issue, a war issue. Yet none of these realms seems equipped to deal with all aspects of a deliberate attack.

A: They're all essential to dealing with it. But none of them has it as their day job.

Q: Should some people have it as their day job?

A: Even if some did, it wouldn't solve the problem. Preventing or responding to a bioattack inherently involves a lot of different communities, none of which can handle all aspects of it alone. It's an example of something we're going to face more and more. There are lots of ways one can imagine doing harm to the United States—whether through infrastructure attacks or cybersecurity or biological attacks—and we can't organize the U.S. government to deal with each and every one of them: There are more problems than there are conceivable government departments. Ultimately, we have to solve the problems we have now and the ones that will come up in the future with the structures we have, and by making sure they're doing the right thing.

Q: How do other nations, both in the developed world and the developing world, perceive this threat?

A: Countries around the world have different priorities. If you have a lot of people getting sick from malaria and TB and HIV, you're not as worried about a potential sprinkling of a couple more exotic diseases as the U.S.—without that ongoing public health burden—would be. They don't see it the same way as we do, although we are getting closer in our approaches

In the early 2000s, conversations between the United States and Europe on this issue reminded me of a scene in Richard Preston's book *The Hot Zone*. Preston wrote about an outbreak of Ebola virus in an animal care facility in Reston, Virginia, at a time when monkeys were dying but it was not yet known that the disease was harmless to people. The Fort Detrick folks come down to the animal care facility, the danger center, and they're mobilizing BSL-4 containment, taping up plastic sheeting and making airlocks. There's a scene in the book where a Ft. Detrick guy is walking down a corridor of the facility in one of these space suits, and he bumps into somebody who worked at the facility who is wearing a T-shirt and blue jeans. They're both looking at each other, and they're both thinking, "*One* of us is crazy."

That's how the U.S. and Europe were talking to each other early on. We were saying the sky is falling, and they were saying, "We don't see the problem."

I think we're making some headway, for 2 reasons. People are coming around to thinking that you can't exclude some of the potential consequences of abusing biology. But the U.S. is also a lot more nuanced in how we go around the world talking about it. We're not saying, "Here is a terrorist threat, you have to drop everything and respond to this brand new problem." We're saying, "There's a range of biological risks. We have existing biosafety issues, we have existing public health issues. We need to talk about that."

The International Health Regulations were a big help. The whole world now knows that we are all responsible for each other's health. And we have some binding regulations, saying all countries around the world need to be able to do X, Y, and Z. If we all develop these capabilities, we will all be in better shape to handle disease, including a biological attack. We're embedding a biosecurity message more effectively

within a public health and a biosafety message today than we did before.

Q: As the new director of the AAAS Center for Science, Technology and Security Policy, what are your plans?

A: I'm thinking: What is it that something with the name "Center for Science, Technology and Security Policy" can't possibly *not* be in the middle of? But my first order of business is not breaking anything. I came into a place that was doing amazing things, including great work in biosecurity.

One of the most important missions I see going ahead is making sure that the scientific community understands, and works well with, the other communities who have to deal with security problems. Here's a story, which is a parody, but has a little bit of truth. It seemed to me that sometime in the late 1990s, when the issue of bioterrorism first came up as a major public policy issue, people in the public health community might have been seen as saying, "We wish these law enforcement, counterterrorism people would just get out of the bioterrorism business. They have no idea what a *disease* is. They're looking for crime scenes and incident sites and red tape and flashing lights, but that's not the way this stuff happens. We know disease; we've been dealing with it all our lives. You don't know exactly where or when it starts; it spreads before you know it's even there. We'll deal with this problem. So, thank you, but get out of our way."

And then across the hall, the law enforcement people are saying, "We wish these public health people would get a clue about bioterrorism. Yeah, we know microbes evolve and they mutate and they change. But they don't read the paper. These people have no idea what an *enemy* is. We understand malicious intent—they've no clue."

So, you had a lot of talking past each other and fingerpointing and saying, "Get out of the way, I'll take care of the problem." But nobody can take care of this problem by themselves. The only way we're going to solve this problem is if everybody understands everybody else's role and respects it. Scientists have to understand what the other communities are trying to do, and these other communities have to understand how science works. That's exactly the kind of conversation we've been trying to facilitate at the Center.

Q: You have argued strongly for bringing back the Office of Technology Assessment, which was closed in 1995. It seems that a vigorous OTA could address a lot of the questions that we've discussed.

A: You're right. If you look at how my current Center was first established by the MacArthur Foundation about 5 years ago, part of the motivation behind it may have been to make up for the fact that Congress no longer had an OTA. I believe it's important to provide S&T advice to Congress. And I support the mission of educating them and providing them with the technical resources they need to do their job. What I resent is the fact that the government is not willing to step up to what it needs to do and therefore looks to private foundations and volunteer experts to make up the difference.

The role of the Center is to make sure that the policy community and the scientific community have as much access to each other as they can. In the absence of the OTA, they may look to us, and we'll do what we can. But we can't be OTA on the cheap.