

**Good afternoon. My intention today is not to be comprehensive with respect to a biological terrorism strategy, but rather to address that part of the problem that has to do with prevention, the focus of this panel.**

**I think there are two points to note at the outset of this discussion about biological terrorism.**

**The first is illustrated by the first slide: around 15 million people, depending on exactly how you do the accounting, die every year from infectious diseases. Infectious diseases are the leading cause of death in the developing world, and a significant cause of death (around fifth or sixth) in the developed world.**

**The 1918 influenza epidemic and the growing risk of avian flu reminds us—as if after AIDS and SARS any further reminders were needed—that global pandemics can have devastating consequences. Any biological security strategy has to address both issues, and take as much advantage of dual-use capabilities—addressing naturally occurring disease as well as possible terrorism—as possible.**

**The second fact to note at the outset is that, historically, there have been very few bioterrorist attacks.**

**We know that Al Qaeda had, and may still have, interest in biological terrorism, although to the extent one can tell from the open literature they seem not to have progressed very far.**

**We know that the Aum Shinrikyo in Japan tried, years before their successful sarin nerve gas attack, to attack Tokyo using anthrax. They failed, and there are lessons to be drawn from that failure. But they did attempt an urban mass casualty attack.**

**And there really are only two other important recent examples, that of the Rajneeshees' salmonella attack in 1984 and the anthrax attacks in fall 2001.**

**It clearly is important to understand the reasons that biological attacks have been so rare. The reasons, I think, involve both capability and intent. One of the themes of my talk today will be that the capability to do dangerous things biologically is growing at a rapid rate, and becoming increasingly available to small groups of the technically competent. This has important implications for terrorism prevention. But it only makes it more important to understand other reasons why so few groups have shown motivation for biological weapons.**

**I currently co-chair the relative threat assessment group in the ongoing Princeton Project on National Security. Our group surveyed nine recent threat assessments, both government and private, going back to just before 9-11. Some of our papers have been posted on the Woodrow Wilson School's website.<sup>1</sup>**

**We were struck at how little attention--in most cases--was paid to motivations compared to attention paid to capabilities. The contrast was striking with George Kennan's famous X article that framed the strategy of containment at the outset of the Cold War—a document that was almost exclusively about motives, rather than capabilities.**

**I share the view expressed earlier in this panel by Jon Wolfsthal and Ash Carter on the many differences between nuclear and biological weapons, and how biological weapons require more attention to response—in the sense of disease surveillance and response. Indeed, in an article in the May**

---

<sup>1</sup> <http://www.wws.princeton.edu/ppns/groups/ThreatAssessment/index.html>

**2002 Foreign Affairs, I contrasted biological weapons with nuclear weapons and cyber threats, arguing that the mix of nonproliferation, deterrence and defense required by an effective strategy against each was so different that lumping them together as “weapons of mass destruction” was more misleading than clarifying.<sup>2</sup> If nuclear weapons are at the left end of a continuum, then cyber “weapons” are at the far right, and chemical and biological fall in between.**

**That is, biological terrorism shares as many or more characteristics with cyberterrorism as with nuclear terrorism. And the trajectory of biotechnology is such that these similarities are only likely to grow—bio is moving closer to the “cyber” end of the continuum.**

**It’s important at this point to distinguish among different levels of concern in the biological realm. Let me delineate five: emerging diseases, state programs, sub-state programs, non-state programs (such as the Aum Shinrikyo), and hackers—this last by analogy to the hackers (often evidently young males) that we’ve become familiar with in the realm of writing or copying and unleashing computer viruses onto the internet, or attacking particular computer or infrastructure systems.**

**Any comprehensive biological security strategy has to address all these levels, and must concern itself with the unintended consequences of a response relevant to one level on all the others. That is, our approach has to have strategic oversight where difficult trade-offs are made—for steps that address one or another of these levels head on may raise dangers in another.**

---

<sup>2</sup> Christopher F. Chyba, “Toward Biological Security,” *Foreign Affairs* Vol. 81, No. 3, May/June 2002, pp. 122-136.

**An important challenge we face in the medium-term future is the challenge posed by the exponentiation of biotechnology. By this I mean that the ability to manipulate organisms to do harm is becoming increasingly available, inexpensive, and automated—at the same time that biotechnology’s advances and spread throughout the world carries enormous promise for advances in public health, food security, and consumer products.<sup>3</sup>**

**The next slide shows the “Kids’ DNA Explorer.” You can order this on the web for \$75; you see it’s for ages 10 and up, and allows—there’s an electrophoresis chamber, for those of you who have taken college molecular biology—your little 10 year old to do rudimentary DNA sequencing.**

**Of course this is just a toy. This next slide is not; it shows a DNA synthesizer—a machine to make short DNA sequences to order—on sail at eBay for under \$3,500. And in case you missed the point, the next slide shows the advertisement that accompanied this machine—“spring blow out clearance sale; like new.”**

**But this too is just an anecdote, and really harmless. It’s this next slide, after a paper by Carlson in 2003 in *Biosecurity and Bioterrorism*, that really shows objectively what’s happening.<sup>4</sup>**

**The slide shows the exponential increase in two types of power—computational power and biotechnological power—through the past few decades. One line shows Moore’s Law,**

---

<sup>3</sup> Much of the discussion throughout this paper of the challenges posed by biotechnology is drawn from Christopher F. Chyba and Alex L. Greninger, “Biotechnology and Bioterrorism: An Unprecedented World,” *Survival* Vol. 46, No. 2, Summer 2004, pp. 143-162.

<sup>4</sup> Robert Carlson, “The Pace and Proliferation of Biological Technologies,” *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* Vol. 1, No. 3, 2003, pp. 203-214.

**the doubling of computer power every 18-24 months. That is, computer power has been exponentiating for several decades, and that is why each of us can have a laptop machine that carries within it vastly more computational power than was available, say, to early nuclear weapons design projects.**

**The other lines show the time required to either sequence or synthesize DNA. The speed at which we can synthesize DNA has also been increasing exponentially. Biotechnology got a later start than computer technology, but this graph shows that it too is increasing exponentially, and with an exponent that is as fast or even faster than Moore's Law in computing. Think of where we were in computing in 1980—we were pretty much all working on big mainframe computers then—and what computing looks like now, 25 years later. That's the kind of qualitative change we'll see in biotechnology in the next 25 years.**

**In particular, I did not imagine in 1980 that some small fraction of high-school and college students would become hackers, capable of writing or copying from websites and modifying computer code to produce viruses that they would then unleash on the internet. As the ability to manipulate microorganisms through biotechnology increases, and as it becomes more and more automated, we may be moving into a world in which biological hacking will become possible. As with computer hacking, much of this will simply piggyback on procedures broadly available on the web or elsewhere.**

**So, for example, with the now-published genome of the 1918 influenza virus, it's possible to synthesize the virus. And what's challenging or cutting-edge today will become commonplace before long, because of the exponentiation of technology.**

**These advances--e.g. determining the genetic code of the 1918 virus and recreating it in the laboratory—will allow terrific advances in fundamental understanding of avian flu viruses--a huge natural threat--and in the rapidity of vaccine production should that be necessary. Other, more exotic defenses will also be enabled.**

**But there is a challenge that comes with this kind of research, in terms of the ability to use technical advances for nefarious purposes as well as defensive purposes. But we should be careful not to suggest that such attacks are somehow inevitable, or that creating pathogenic organisms in the lab will be easy. The Aum Shinrikyo and Al Qaeda did not find it so, and modifying an organism to be pathogenic, and being confident that the organism is pathogenic will require a testing program—the sort of program that will be far more likely to be detected than bench research itself. And, you have to do all this without killing yourself and your colleagues.**

**Finally, as we devote substantial resources to defensive measures intended to help protect ourselves against what might be cooked up in some offensive-minded state or terrorist program, we need to weigh extremely carefully the overall impact of our approach, and the possibility that, if misperceived, it could feed the very kind of state-driven biological arms race that we all have an interest in ensuring never again threatens the world.<sup>5</sup>**

**It would prove difficult for a non-state group or individual hacker to produce large quantities of weapons-grade, aerosolizable material that could cause mass casualties without involving a contagious organism. And ultimately, any release**

---

<sup>5</sup> These concerns were discussed in greater length in Christopher F. Chyba and Alex L. Greninger, “Biotechnology and Bioterrorism: An Unprecedented World,” *Survival* Vol. 46, No. 2, Summer 2004, pp. 143-162.

**of a highly virulent contagious organism would hurt much of the rest of the world far, far more than any developed-world city that may have originally been its target.**

**I'll end by noting that, as with nuclear weapons, there is no "silver bullet" solution to our problem. We have to rely on a web of prevention, where each strand of the web is clearly inadequate in itself. We have to be conscious of the fact that strengthening some strands in the web may weaken others, and make strategic decisions about how to proceed. And any effective approach will necessarily include a strong international component.<sup>6</sup>**

**In this context, the implementation of UN Security Council Resolution 1540, which requires all countries to criminalize biological weapons development by non-State actors, as well as to adopt appropriate measures to safeguard the most dangerous pathogens, is a step in the right direction.**

**In closing, I'll take advantage of Congressman Schiff's presence on our panel today, to note that the Global Pathogens Surveillance Act, which has passed the Senate but has never come up for a vote in the House, would be another very good step in the right direction. Thank you.**

---

<sup>6</sup> This discussion is taken from Christopher F. Chyba and Alex L. Greninger, "Biotechnology and Bioterrorism: An Unprecedented World," *Survival* Vol. 46, No. 2, Summer 2004, p. 147.