Preventing the misuse of gene synthesis

To the Editor:

As representatives of two companies—GENEART and DNA2.0—that together are responsible for a majority of the world's manufacture of synthetic genes, we feel compelled to respond to Nouri and Chyba's proposition for "proliferation-resistant biotechnology," as published in the March issue[1]. Gene synthesis enables a new world of possibilities: in the development of biofuels to combat climate change, in drug development to combat both persistent and emerging diseases, in agriculture to engineer crops that are more nutritious and resilient, and in research to bring a deeper understanding of the inner workings of the cell and of life itself. Biosafety and biosecurity are of utmost importance to us; even a small breach in biosecurity could damage the reputation and stability of our companies and our mission to facilitate the research that will bring solutions to the critical problems of the twenty-first century. We have the greatest incentive to ensure that the genes we synthesize do no harm and that the practice of gene synthesis remains safe.

Nouri and Chyba envision "the diffusion of advanced synthesizers from a few centralized locations to an increasing number of facilities and perhaps even individual laboratories…" as a result of "new and innovative approaches and declining development costs." They suggest equipping such synthesizers with software to block the synthesis of potentially harmful gene sequences. We counter, however, that their strategy is an ineffective way to increase public safety for several reasons.

First, the cat is already out of the bag. Gene synthesis has been around for a quarter of a century, and scarcely a month goes by without a new protocol being published[2]. Using web-based design tools[3] and PCR-based protocols[4,5], gene synthesis can already be practiced in any lab, or even a startup garage if time and money are no object. Anyone who is sufficiently motivated could synthesize the gene for a toxin or even an entire viral genome[6] using readily available reagents and without ever going near a specialized synthesizer.

Second, there are often legitimate reasons in the interest of safeguarding human populations for synthesizing genes that encode parts of toxins and harmful viruses, for example, as therapeutics[7] or as sources of antigens. Synthesis of these genes would require protocols for bypassing the dangerous-sequence block on the synthesizers, further increasing the ease with which hackers could evade these controls. Nouri and Chyba do acknowledge the need for certain scientists and laboratories to have access to select agents, and they recommend that a special software patch would be granted to those that have clearance. Whatever solution is used to bypass the block thus creates a vulnerability that would most certainly be exploited by terrorists or organizations serious about causing destruction.

Third, gene synthesis appears to be an unlikely tool for anyone seriously considering harm. Why would a nefarious agent bother with the expense and expertise required for synthesis when it would be much easier to find *Bacillus anthracis* in any pasture land? Why would a terrorist risk the exposure of attempting to order a dangerous sequence from a synthesis company—which would still require significant laboratory expertise to transform into a viable agent—when so many other conventional methods for causing harm are readily available?

Despite the unlikelihood that DNA synthesized commercially would be used for bioterrorism, we have adopted an effective procedure for ensuring that dangerous synthesized sequences do not fall into the wrong hands, a process that both GENEART and DNA2.0 currently implement with all their orders. On the basis of select agent lists from the US Centers for Disease Control and Prevention, the US Department of Agriculture (http://www.selectagents.gov/) and the Australia Group (http://www.australiagroup.net/), we have compiled a list of sequences against which we screen all incoming orders. We do not produce or ship genes that match any sequence on this list without an official permit[8].

This protocol has several advantages over Nouri and Chyba's suggestions. It is effective immediately and does not have to await a distant future when gene synthesis is so perfectly automatable that punching a few keystrokes into a computer will pop out the Spanish flu virus. By screening against a list of restricted sequences within the company, rather than exposing sensitive or proprietary sequences to a transparent system, we can ensure that laboratories and researchers feel secure enough to utilize our services. If customers suspected that the confidentiality of their sequences might in any way be compromised, we would witness a withering of the enormous amount of innovation currently facilitated by synthesis; it could even compromise our ability to respond to potential pandemics[9].

Although we stand behind our self-imposed regulation, there is no doubt that the government could act to improve its efficacy. For this reason, we call upon both the United States and Europe to require all makers of synthetic genes to screen according to a list of restricted sequences compiled by the relevant experts. We have done our best to craft a screening list, but we believe that our governments should be able to provide the most up-to-date and accurate list of restricted sequences.

Equally important to a comprehensive screening list is a plan for enforcement. We believe that our governments should routinely test all synthetic gene makers for compliance to the list. In this way, any irresponsible gene manufacturers can be immediately shut down. By routinely attempting to order dangerous sequences from laboratories outside of Europe and the United States, we can have an effective surveillance program even if we are not able to get international agreement on regulations such as proposed by the Australia Group. Whether through governmental channels or the world media, gene makers who act irresponsibly will not be able to continue to operate profitably. As we have seen recently in regards to food safety, international attention to contaminated food originating in China provoked an immediate shift in consumer behavior and, in turn, swift action by the Chinese government to crack down on irresponsible companies.

This is a time in our history when gene synthesis offers considerable assistance in tackling the mounting pressures of climate change, a burgeoning world population and pertinacious disease. Furthermore, gene synthesis provides scientists with valuable tools to find solutions to bioterror itself, facilitating the development of vaccines and diagnostic antibodies without requiring the culturing of active pathogens. By implementing a simple, sane regulation and enforcement policy regarding gene synthesis,

we can head off the possibility that synthesized genes could be used to cause harm. We do not find any value in resorting to science fiction fantasies to foment fear about the process of gene synthesis. In our view, this endangers the very industry that will generate important solutions for our present problems while obscuring the true threats to our security.

COMPETING INTERESTS STATEMENT
The authors declare competing financial interests: details accompany the full-text HTML version of the paper at http://www.nature.com/naturebiotechnology/.

Jeremy Minshull[1] *& Ralf Wagner*[2]

[1]*DNA2.0, Inc, Menlo Park, California, USA.*
[2]*GENEART, Regensburg, Germany.*
e-mail: jminshull@dna20.com

1. Nouri, A. & Chyba, C.F. *Nat. Biotechnol.* **27**, 234–236 (2009).
2. Czar, M.J., Anderson, J.C., Bader, J.S. & Peccoud, J. *Trends Biotechnol.* **27**, 63–72 (2009).
3. Hoover, D.M. & Lubkowski, J. *Nucleic Acids Res.* **30**, e43 (2002).
4. Xiong, A.S. *et al. Nat. Protoc.* **1**, 791–797 (2006).
5. Reisinger, S.J., Patel, K.G. & Santi, D.V. *Nat. Protoc.* **1**, 2596–2603 (2006).
6. Cello, J., Paul, A.V. & Wimmer, E. *Science* **297**, 1016–1018 (2002).
7. FitzGerald, D. & Pastan, I. *J. Natl. Cancer Inst.* **81**, 1455–1463 (1989).
8. Bügl, H. *et al. Nat. Biotechnol.* **25**, 627-629 (2007).
9. Song, L. *et al. PLoS One* **3**, e2257 (2008).

Chyba and Nouri reply:

Concerns about the possible misuse of gene synthesis in particular and biotech more generally are not "science fiction fantasies," but rather a legitimate cause for concern. Attempts to address these concerns must be carefully balanced against the extremely important benefits that flow from these technologies, as we emphasize in the first paragraph of our Commentary[1]. The seriousness of the possible misuse of these technologies has been addressed by two National Academy of Sciences committees[2,3], and in a workshop held by the Royal Society and the International Council for the Life Sciences[4]. (For full disclosure, one of us was a member of one of these Academy committees and a participant in the Royal Society workshop that led to the new report.)

Minshull and Wagner criticize our suggestions on three grounds: first, the "cat is already out of the bag" and "anyone who is sufficiently motivated" can already synthesize genes "or even an entire viral genome"; second, the requirement that legitimate users be able to readily bypass any controls will permit "hackers" to bypass these controls; and third, gene synthesis is "an unlikely tool for anyone considering harm" because there are so many other biological and conventional means to cause harm. We acknowledged these objections but did not find them sufficient to mean that nothing should be done.

What is striking is that, despite their rhetoric, Minshull and Wagner obviously agree with us on this. They themselves summarize the controls that their companies, and others, have placed on gene synthesis, based on the select agent lists. They require official permits for certain genes to be produced or shipped. Moreover, they call upon governments in the United States and Europe to "require all makers of synthetic genes to screen" synthesis orders. So, in fact, there is no disagreement in principle between their viewpoint and ours; the difference exists in the specifics of its application.

There is no silver bullet that will somehow solve the security challenge of dual-use biotech. Rather, we must implement a web of measures, carefully calibrated so as not to impede legitimate and lifesaving research, that will make it more challenging—not render impossible—the casual or even dedicated misuse of this technology. The hope is that such misuse will be challenging enough that any individual or group contemplating it will choose an altogether different approach to doing harm. But were the technology to become both extremely easy to use and widely available, further steps might be required to help ensure these favorable outcomes.

We do not suggest that gene synthesis companies drop their controls; in fact in our Commentary we applaud the steps that have been taken. Our concern, rather, lies with a possible future—whose trajectory can already be discerned—in which automated DNA synthesis machines diffuse to a large number of users. In this case, additional proposals beyond those applicable to central providers must be considered. Our suggestions, like those implemented by Minshull and Wagner, build on the select agent list and, like theirs, would require some permit structure for the synthesis of especially dangerous sequences which, like theirs, introduces some vulnerability to misuse that must be managed. In effect, we simply recommend extending their practices to a new technology. Given their call for greater government requirements along these lines for their own industry, we are puzzled why they object to our suggestions.

1. Nouri, A. & Chyba, C.F. *Nat. Biotechnol.* **27**, 234–236 (2009).
2. National Research Council. *Biotechnology Research in an Age of Terrorism: Confronting the 'Dual Use' Dilemma* (National Academies Press, Washington, DC, 2003).
3. Committee on Advances in Technology and the Prevention of their Application to Next Generation Biowarfare Threats. *Globalization, Biosecurity, and the Future of the Life Sciences* (National Academies Press, Washington, DC, 2006).
4. Science Policy Centre. *New Approaches to Biological Risk Assessment* (The Royal Society, London, 2009).

Commercialized GM crops and yield

To the Editor:

A News article in the July issue[1] brings up some important questions about our report, *Failure to Yield*, which analyzes the contribution of genetic engineering to increased food and feed production in the United States, and its potential for contributing to global food security. I would like to clarify some points by responding to some of the comments made by several researchers interviewed in the article.

We do not recommend that genetic engineering be scrapped in favor of conventional breeding—the main complaint of Jonathan Jones. We note in the executive summary: "Genetic engineers are working on new genes that may raise both intrinsic and operational yield in the future, but their past track record for bringing new traits to market suggests caution in relying *too heavily* on their success" [emphasis added][2]. We should favor methods that have been, and continue to be, more successful at increasing productivity, such as conventional and genomics-assisted breeding—this does not mean eliminating genetic engineering.

Our report relied heavily (but not exclusively) on US field trials to derive yield values for genetically engineered traits. Field trials allow the comparison of crop treatments, while holding other variables relatively constant. This allows the testing of the yield contribution of a transgene—which was a goal of our report. Field trials are conducted under ambient