From synthetic biology to biohacking: are we prepared?

Gaymon Bennett, Nils Gilman, Anthony Stavrianakis & Paul Rabinow

The emergence of synthetic biology, and off-shoots such as DIYbio, make the need for a rigorous, sustained and mature approach for assessing, and preparing for, the broad range of associated dangers and risks all the more pressing.

In the past year, a spate of articles has reported on the growth and formalization of 'DIYbio'[1–7]. Alternately portrayed as techno-progressive, rogue and, above all, hip, this global cadre of DIYbio practitioners or biohackers is stylized as being capable of doing at home what just a few years ago was only possible in the most advanced university, government or industry laboratories[8]. The degree to which such capabilities have been, or can be, actualized remains an open and empirical question. What is clear is that the emergence of DIYbio and synthetic biology add urgency to the creation of a framework for systematically evaluating the risks and dangers of biological engineering. To proceed in that direction, more sustained reflections on the problems and objects at issue is a mandatory prerequisite.

Given the increasing ease and availability of biological engineering, the community needs to spend more time and effort in assessing and anticipating the dangers and risks associated with the technology.

DIYbio versus synthetic biology

The media attention surrounding DIYbio has served to brand the endeavor just as synthetic biology was branded. Both embrace the goals of making biology 'easy to engineer' and ensuring materials and know-how circulate in an 'open source' mode—"biology for the people" as the platitude has it. The association is not surprising or accidental. DIYbio and synthetic biology, after all, share institutional and personal connections. Leading research institutions, such as the National Science Foundation–funded Synthetic Biology Engineering Research Center, of which three of us (P.R., G.B. and A.S.) are a part, have made these two goals central to their strategic plans. Additionally, leading figures in synthetic biology have informally served as impresarios to some in the biohacker movement, notably through their sponsorship and promotion of the International Genetically Engineered Machines (iGEM) competition, which in 2009 has drawn over 100 teams of undergraduate bioengineers from five continents. In the light of the growth of DIYbio and the publicity that it has generated and received, however, the directors of the iGEM competition have banned DIYbio teams from participating in the competition.

The connections and convergences can no doubt be overstated. Self-definitions vary, and not all synthetic biologists would define their field as fostering "mechanisms for amateurs to increase their knowledge and skills," as a prominent DIYbio website (http://diybio.org/) puts it. Conversely, not all DIY biologists design "new biological parts, devices, and systems," as synthetic biology has sometimes been defined (http://syntheticbiology.org/). Nevertheless, it's certainly fair to say that accessible, easy-to-engineer biology is becoming the proverbial name of the game. Those synthetic biologists and DIYbio practitioners who object to being grouped together need to speak up in their own name.

The good news is that open access biology, to the extent that it works, may help actualize the long-promised biotechnical future: growth of green industry, production of cheaper drugs, development of new biofuels and the like. The bad news, however, is that making biological engineering easier and available to many more players also makes it less predictable, raising the specter of unknown dangers.

Biosecurity issues

A range of researchers and research institutions have raised the issue of biosecurity.

Gaymon Bennett, Anthony Stavrianakis & Paul Rabinow are at the Synthetic Biology Engineering Research Center and the Department of Anthropology, University of California at Berkeley, Berkeley, California, USA. Nils Gilman is at Monitor 360, San Francisco, California, USA.
e-mail: gaymon.bennett@berkeley.edu

Two different consortia of companies, for example, have proposed competing screening frameworks to deal with new capacities in biosynthesis technology[8]. The trouble with many of these responses, however, is that they take the increase in technical capacities, *per se*, to basically be the heart of the matter[9]. Ergo: technical solutions are proffered as adequate to technical problems. This technical approach is framed as 'dual use': there are good uses and bad uses, good users and bad users. Given this frame, a double challenge is posed: how to either design things biological, such that the 'bad guys' can't reengineer what the 'good-guys' have made, or set-up screening procedures so that the good guys can effectively keep the bad guys out. The goal: prevention through technical and organizational blockage.

> What is clear is that the conditions of the life sciences have changed dramatically since the 1975 conference on recombinant DNA at Asilomar.

Such responses no doubt have their place. The trouble is these responses don't actually address the problem at hand (leaving aside the intractable difficulty of discerning who is good and who isn't). The real concern in all of this is the fact that dangerous events, whether intentional or accidental, are facilitated through an increase in ease and access. Much to their credit, the authors of the widely circulated Sloan report[10] on synthetic biology and biosecurity have made this same point.

To the extent that more and more people in less and less formal and visible settings are able to engineer biological systems, the possibility of predicting the form and timing of such dangerous events, and thereby preventing them, becomes intractable. In certain respects, DIYbio is a 'black swan' waiting to happen: it portends events whose probability might seem low, but whose negative impact is likely to be quite high[11].

The insufficiency of current responses is reflected in, and reinforced by, a trend toward polemics. On one side, there are activists, such as those that form the Canadian nongovernmental organization, the Action Group on Erosion, Technology and Concentration, who evoke the 'precautionary principle'. These activists want to shut down all research programs for which the range of negative outcomes cannot be reliably determined in advance. Given that science, by definition as well as practice, is experimental in character, such a position amounts to shutting down bioengineering altogether, whether synthetic biology, DIYbio or otherwise[12].

On another side, there are enthusiasts, practitioners of synthetic biology, and biohackers. Enthusiasts subscribe to what has been called a 'proactionary principle', which invokes a 'right to innovate'[13]. Enthusiasts are often unwilling to frankly address dangers posed by easy-to-engineer and open-source biology. To the extent that such possible dangers are acknowledged, an attitude of 'trust us' pervades. Enthusiasts and entrepreneurs are willing to concede the need for some forms of indirect self-regulation. Policymakers, however, should leave it to the biologists to develop norms and protocols.

Polemics may not be strictly representative. They are, however, consequential. These polemics introduce a shell game in which the facts of the matter hide under one analogy after another, each coming in quick succession. Synthetic biology, activists say, is just like giant agribusiness. It's really all about ownership of nature, destruction of biodiversity and devastation of marginalized farming communities. Or, maybe it's Frankenstein that should worry us. Garage biologists will create designer organisms, fashioned to the maker's will. The implications are familiar: violated nature will reap its own revenge.

On the other side, enthusiasts use a Lego analogy: bioengineering will be made child's play; order your kit and get to work. Or, when addressing a more skeptical audience, the analogy becomes the computer industry: yesterday, we were building PCs in our garages; today, we have iPhones. Message: if you want your iPhone, put up with the potential for the equivalent of a few computer viruses. The only trouble is that the analogy between computer viruses and bioengineered viruses is not at all apt: computer viruses can't kill people, at least not directly.

What gets covered over by activists and enthusiasts alike is that the contemporary admixture of bioengineering and biosecurity forms a combination with distinctive and distinctively troublesome characteristics. It's safe to bet that synthetic biology and DIYbio will only intensify these characteristics. The point is that today, we've got a distinctive problem on our hands; attending to its particularities is a demand of the first order.

The taken-for-granted credibility of Asilomar-like self-governance, as some senior researchers have recognized, is highly contestable and does not stand up to critical evaluation. The organizers of the annual 'SynBio' conferences, for example, have invited scrutiny and criticism from nonengineers and nonbiologists. And the charter for the National Science Advisory Board allows the participation of nontechnical experts. Whether this is a mere gesture or will contribute to better governance remains to be seen.

What is clear is that the conditions of the life sciences have changed dramatically since the 1975 conference on recombinant DNA at Asilomar. The exclusion of the public is no longer even imaginable in the age of the internet. Gentleman's agreements of a kind that were common in 1975 are no longer imaginable, given the rise of patenting in the biotech industry. Assurances by patriarchs that safety issues can be handled through expertise and containment are no longer plausible given the global conditions of security. And so on.

It follows that, among other things, safety by design and screening technologies alone won't cut it. Technical capacities are increasing, to be sure. And these technical capacities need to be responded to at a technical level. But such a task, difficult and worthwhile as it may be, is only one vexing aspect of the current situation. The increase in technical capacities is just a first vector that makes the current problem distinctive and troublesome. Here are some others that warrant careful reflection:

- Moral arrogance. Many elite researchers and self-styled hackers tacitly concur that all technical advance is worthwhile and that only malicious people will do bad things. Arrogating moral goodness to the bioscientific side of the ledger overly simplifies a moral landscape that needs to be analyzed in all its complexity and contradiction.

- New actors and actions. The post-9/11 security environment is characterized by new actors and actions. For the past eight years, US citizens have had to face what most of the rest of the world has confronted daily for some time: that the difference between who and what is dangerous, and who and what is not, is a blurred and ever-shifting matter.

- Existing global access. Global capital and the internet have taken cutting-edge biology into laboratories around the globe. Even without DIYbio, bioengineers in countries all over the world have access

to materials and know-how. If Iran can fund developments in nuclear technology, they can certainly foot the bill for a few synthetic biology laboratories.

- Shifts in governance. For a decade now, national and multinational regulators and planners have increasingly been turning their attention to 'low-probability/high-impact' events rather than civil defense. Preparedness for such events, whether 9/11, Hurricane Katrina or H1N1 flu, seems to be the order of the day everywhere but in the laboratories and fraternities of advanced bioengineering.

All told, facilitating DIY capabilities for designing and constructing biological systems makes all of these factors even more difficult to deal with, to say the least.

Another approach

We argue that developments in synthetic biology and DIYbio call for another approach. Beyond the denunciation of the activists and the hype of enthusiasts, we need the vigilant pragmatism of what we have called 'human practices' (http://www.synberc.org/humanpractices). Such an approach consists of rigorous, sustained and mature analysis of, and preparation for, the range of dangers and risks catalyzed by synthetic biology and DIYbio. Preparedness activities might include on-the-ground tracking of the ramifications of synthetic biology research, or training in emergency response to biological events. Less familiar activities might include scenario development and stakeholder war-gaming (e.g., see http://www.gbn.com/; http://360.monitor.com/).

In the coming years, the intertwined growth of synthetic biology and DIYbio will further limit the scope of the current 'dual-use' framing of biological threat assessment and mitigation based on guarding key facilities, establishing export controls and monitoring technical experts. In its stead, policy makers will need to develop new analytic and policy frameworks, frameworks calibrated as much to preparation for unlikely but damaging events as to the design of technical safeguards[14].

We simply do not know the full extent of dangers on the near-future horizon, or of opportunities for that matter. We cannot be certain how biotechnological capacities will expand and ramify. We cannot be certain of the extent to which synthetic biologists and biohackers will successfully make biology easy to engineer or open source. We can be certain, however, that the stakes are high for everyone involved—above all for the enthusiasts. Those unwilling to prepare for dangerous events are exposing themselves, professionally and personally: if and when an untoward bio-event takes place, the so-called experts who failed to prepare will take the lion's share of collective blame. Studies, laboratories and careers are likely to be policed or even terminated.

The central challenge today is to neither shut things down, nor simply trust the experts. Rather, the challenge is to foster sustained and engaged inquiry that takes the pragmatic conditions of this techno-science and its practitioners as its primary object of concern, rather than hype or fear about an imagined future. Following this human practices mode, we might be able to anticipate and specify how to prepare regulations, normative frameworks and ethical responses adequate to the demands of the day.

AUTHOR CONTRIBUTIONS

All authors contributed equally to the work presented in this paper. P.R. directed the work of the Berkeley research team. N.G. conducted primary research on DIYbio. G.B. was the lead writer. A.S. was a secondary writer. All authors discussed and revised the manuscript at all stages.

1. Johnson, C.Y. Hackers aim to make biology household practice. *Boston Globe* September 15, 2008.
2. Degasne, S. ADN: les biohackers créent des monstres dans leur garage. *Rue 89* November 3, 2008.
3. Anonymous. Biohackers attempt to unstitch the fabric of life. *Associated Press* December 27, 2008.
4. McKenna, P. The rise of the garage genome hackers. *New Scientist* January 7, 2009.
5. Bloom, J. The geneticist in the garage. *The Guardian* March 19, 2009.
6. O'Brien, D. Hacking into the building blocks of life itself. *Irish Times* April 10, 2009.
7. Whelan, J. In attics and closets, 'biohackers' discover their inner Frankenstein. *Wall Street Journal* May 12, 2009.
8. Hayden, E.C. *Nature* **461**, 22 (2009).
9. Nair, N. *Nat. Med.* **15**, 230–231 (2009).
10. Garfinkel, M.S., Endy, D., Epstein, G.L. & Friedman, R.M. *Synthetic Genomics: Options for Governance* (J. Craig Venter Institute, The Center for Strategic and International Studies, Massachusetts Institute of Technology, October 2007). http://www.jcvi.org/cms/fileadmin/site/research/projects/synthetic-genomics-report/synthetic-genomics-report.pdf
11. Taleb, N.N. *The Black Swan: The Impact of the Highly Improbable* (Random House, New York, 2007).
12. http://etcgroup.org/upload/publication/602/01/synbioreportweb.pdf
13. Schmidt, M. *et al. Syst. Synth. Biol.* **2**, 7–17 (2008).
14. Ostfield, M.L. Biosecurity Bioterrorism: Biodefense Strategy, *Practice Sci.* **6**, 261–267 (2008).