Proliferation-resistant biotechnology: an approach to improve biological security

Ali Nouri & Christopher F Chyba

Is there a way to design DNA synthesis technology with safeguards that prevent its cooption for nefarious purposes?

To prevent the application of pathogenic genes and genomes to the production of biological weapons, some commercial DNA providers now screen orders so that potentially dangerous sequences are not synthesized. However, new and innovative approaches and declining development costs could enable the diffusion of advanced synthesizers from a few centralized locations to an increasing number of facilities and perhaps even individual laboratories, rendering the current risk-management framework obsolete. To prepare for this possibility, we propose the development of 'proliferation-resistant biotechnology'—safeguards intrinsic to emerging technologies that will ensure that nefarious applications are hindered while benefits are preserved. As biotechnologies become increasingly automated, such safeguard strategies can become effective tools for managing risks in the life sciences.

©Andrew Brookes/Corbis

As DNA synthesis technology increases in power, proliferation-resistant approaches should be incorporated to prevent its cooption for nefarious purposes.

Emerging technologies

Biotechnological advances underlie a scale and pace of biological research never before seen. Plunging DNA sequencing costs have made a $1,000 human genome a realistic goal. *De novo* DNA synthesis technologies now automate the assembly of long DNA molecules from sequence data alone. Just recently, the J. Craig Venter Institute (Rockville, MD) announced the chemical synthesis of a minimal bacterial chromosome—over half a million nucleotides[1]. Further cost reductions for this technology may transform molecular biology, resulting in the replacement of conventional gene cloning techniques by automated DNA synthesis. But the technology is dual use: although beneficial for biological research, it can also be applied toward the production of biological weapons by states, non-state groups and even individuals. For instance, many viral genomes have been sequenced; these are typically small and well within the limits of commercial DNA synthesis. High-profile scientific publications have already demonstrated the application of *de novo* DNA synthesis to the creation of the poliovirus[2], as well as the otherwise extinct Spanish influenza virus[3]—the agent that is estimated to have killed around 50 million people in the pandemic that began in 1918.

Although DNA synthesizers can be readily purchased, using these to build large genes and viral genomes is technically challenging and time-consuming and requires considerable material. At the same time, these DNA molecules can be obtained almost effortlessly, within days or weeks, from commercial entities that employ more advanced technologies. These DNA providers are aware of the risks,

Ali Nouri is currently an AAAS Science Policy Fellow in the office of US Senator Jim Webb. He was and Christopher F. Chyba is at the Program on Science and Global Security, Woodrow Wilson School of Public and International Affairs, Princeton University, Princeton, New Jersey 08544, USA.
e-mail: nouri@princeton.edu

and, to protect against illicit acquisition of sequences that could subsequently be transcribed and translated into infectious agents, some have begun to regulate themselves. In the United States, these procedures include screening all incoming DNA orders so that genomes and genes of federally regulated pathogens and toxins, respectively, are not synthesized (except for researchers permitted to work with these regulated agents)[4–6]. These voluntary measures are likely to be formalized into mandatory ones; the major US biosecurity panel, the National Science Advisory Board for Biosecurity (Washington, DC), has called for governmental oversight of commercial DNA synthesis[7].

These regulatory schemes may help to prevent the misuse of commercially provided DNA molecules, but they will only be effective so long as the underlying technologies remain centralized at a relatively small number of facilities. Meanwhile, increasing demand has made large-DNA synthesis a competitive area, resulting in the development of multiple platforms[8–10], all of which have potential for automation. One possible outcome of this could be the diffusion of more advanced synthesizers to large numbers of users, making the current risk-management framework increasingly irrelevant. To prepare for this possibility, alternative nonproliferation proposals need to be explored.

Conventional nonproliferation strategies

An important consideration for nonproliferation strategies in any dual-use area is that the efforts not unnecessarily hamper the technology's benefits. This is especially true for biotech, which has critical implications for improving human health and agriculture. What makes this an even greater challenge is that the biological research process—whether legitimate or nefarious—lacks obvious bottlenecks that might be amenable to safeguards.

This is profoundly different from the situation with nuclear energy, where nonproliferation strategies take advantage of the fact that paths toward nuclear weapons pass through the severe bottlenecks of either highly enriching uranium, or producing and reprocessing plutonium. These bottlenecks serve as the basis for the extensive monitoring that underlies the nuclear nonproliferation regime. As a recent illustration, consider the monitoring conducted by the International Atomic Energy Agency (IAEA) at the Chinese gas-centrifuge uranium enrichment plant at Shaanxi. The IAEA installed into this facility equipment that monitors the uranium flow rate and enrichment levels, to "provide continuous unattended monitoring of enrichment levels and quantity of the product"[11]. Any efforts to divert uranium, or enrich it beyond the level appropriate for peaceful use, would thereby be automatically detected.

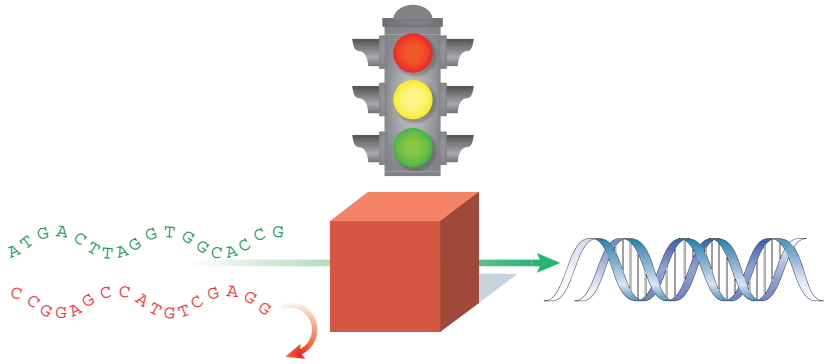

Figure 1 Proliferation-resistant biotech. Advanced biotechnologies, such as DNA synthesis, are becoming increasingly automated and black boxed, providing even novice researchers with powerful tools. This automation, however, also provides an opportunity to incorporate intrinsic safeguards that block illicit sequences (red) from being synthesized, while allowing legitimate ones (green).

This difference between most industrial-level nuclear processes and laboratory biotech guarantees that many analogies between nuclear and biological nonproliferation strategies fail badly and that very different approaches are needed for the two cases[12]. Meeting the challenge of biotech requires a web of measures, most of which little resemble the approaches deployed to prevent nuclear proliferation[13]. Nevertheless, an important strand in this web of prevention may prove to be nonproliferation measures—but only if appropriately conceived.

Rather than depending on any industrial-scale bottleneck processes analogous to those needed to produce weapons-useable nuclear material, biotech predominantly relies on skilled, knowledgeable individuals who employ readily available tools and even renewable reagents (such as bacterial-derived restriction enzymes or competent bacteria for transforming DNA). The lack of obvious intervention points has left the life sciences with overly broad nonproliferation proposals of a restrictive (for example, curbing access to technologies and know-how) or intrusive nature (for example, physical inspections of laboratories that conduct biological research)[14].

There are legitimate concerns, however, that restrictive or intrusive nonproliferation proposals will hurt scientific progress, as well as hindering robust responses to any disease outbreak, whether natural or intentional. So instead, proposals of a softer nature have gained traction. For example, through the Biological Weapons Convention, countries have come to rely on self-reporting of research activities, increased awareness-raising and the adoption of codes of conduct as primary mechanisms by which dual-use biotech is addressed. Although these strategies are essential for establishing and strengthening norms against misuse, by themselves they cannot prevent any aspiring illicit actor. Proliferation-resistant technologies could begin to fill this gap.

Proliferation resistance

Proliferation-resistance strategies arose as a way to help manage dual-use nuclear technologies. Such intrinsic safeguards are intended to hinder the diversion of technologies for weapons-grade nuclear material production while allowing the peaceful applications of the technology. Currently, life science tools are undergoing rapid transformation, from manual technologies to ones that are increasingly automated. This automation provides an opportunity to incorporate safeguards into the technologies themselves, so that only their nefarious applications are hindered. In the case of DNA synthesis, for instance, safeguards could include the implementation of DNA screening software into synthesizers so that a subset of sequences, such as toxins and pathogen genomes, cannot be illicitly synthesized (**Fig. 1**). To determine the set of sequences that would be disallowed, a pre-existing regulatory framework that applies to the possession of pathogens and toxins of concern could be extended to their DNA sequences. In the United States, for instance, possessing these agents of concern requires licensing by the Centers for Disease Control and Prevention or the Department of Agriculture. Sequencing discrimination would be more challenging for genetic material that is very similar, but not identical, to agents of concern, such as those belonging to particular vaccine strains. Any

future regulatory framework that attempts to extend licensing procedures from pathogens and toxins to their sequences would have to address this, perhaps by restricting sequences that cross a certain threshold and become too similar to an agent of concern.

For researchers who would be registered to perform experiments with the genetic material of agents of concern, a software update (such as a downloadable patch) could be obtained to bypass certain restrictions. Just as US federal law prohibits the transfer of these agents of concern to unauthorized users, software updates and patches could follow a similar regulatory framework, while also incorporating requirements specific to individual machines. To account for regulatory changes, such as those needed to address novel pathogens or toxins, software could be updated on a regular basis.

Detection of illicit activity by users might be accomplished if synthesizers were designed to operate only when online, in a transparent manner whereby any software manipulation would be revealed to the online community. This approach does have some drawbacks, such as increasing access and, thus, vulnerability of synthesizers to the online community. These concerns could be alleviated in part via stronger schemes that might include the incorporation of computer chips into synthesizers to block the production of certain sequences. Moreover, because biotech advances tend to outpace the government regulatory process, data chips or even synthesizers could be regularly modified or replaced with improved versions that were also updated to comply with any changes to the regulated list of pathogens and toxins.

This system of DNA synthesis screening at the machine level would not replace the university and agency-level human experiment review that occurs in some countries but would rather complement it as another strand in an overall web of prevention.

These approaches might also be applied more broadly to other emerging biotechnologies, such as some in the fledgling field of proteomics. The *de novo* synthesis of amino acids from chemical precursors, for instance, enables construction of proteins of around 300 amino acid residues in size—putting a number of human protein toxins well within reach. The technology lowers required expertise in molecular biology and biochemistry techniques, enabling a relative novice to construct proteins of any sequence with any desired amino acid modifications, which can further influence protein activity. Similar to *de novo* DNA synthesis safeguards, screening software could be employed in future automated protein synthesizers to prohibit the construction of particular toxic gene products.

A concept analogous to these strategies might be found in the V-chip, a feature that can block the display of television programming of a particular rating. The V-chip, however, is intended only to exert parental control over television viewing and can easily be reprogrammed and even disabled. In the case of dual-use biotechnologies, such security measures would require more stringent criteria along the lines discussed above.

The way forward

Proliferation-resistant safeguards could be designed during the initial development of new technologies. A way to achieve this is to create incentives through special funding for innovators. Since the 2001 mail anthrax attacks, the US federal government has spent over $40 billion just on civilian biodefense projects[15]. A large portion of this is dedicated to developing countermeasures (such as vaccines and drugs) and surveillance and detection tools, but to our knowledge, virtually no funding is allocated for developing biotechnologies that are intrinsically more secure. Designing and deploying these would help to prevent misuse of the technology, thus relieving some of the need to develop measures aimed at neutralizing laboratory-generated pathogens.

Deploying proliferation-resistant biotechnologies first requires that rules for possessing organisms and toxins of concern be extended to their genetic sequences. A greater challenge, however, will be to extend these rules internationally. Many countries lack a regulatory framework for dealing with such agents, let alone their genetic material. And for those that do have a framework in place, perceived biological threats vary greatly, leaving many challenges to the creation of a harmonized global framework. Given the international dimension of life science research, however, any comprehensive biological security strategy should be international in scope and should include improved rules for the possession and sharing of biological agents—and their genetic material—both within and among nations. Finally, by themselves, the technical safeguards discussed here will not alleviate all the risks that arise from the illicit genetic engineering of pathogens and toxins. Rather, these safeguards should be regarded as one component that, together with other measures, constitute a web of prevention[13] to reduce the likelihood of production and deployment of biological weapons.

Although certain advanced biotechnologies still occupy a niche market, declining costs will make them increasingly dominant. Conventional molecular biology techniques that are used to construct and manipulate DNA molecules, for instance, are likely to eventually be replaced by the faster, cheaper and almost effortless *de novo* synthesis. As these new automated technologies begin to replace older, manual ones, there is an opportunity to introduce proliferation-resistant safeguards into the newer generation of biotechnologies. Gradually, improved automated technologies that are also safeguard-friendly will replace the older, less efficient and difficult-to-safeguard tools. This means that, if managed properly, the revolution in synthetic biology need not increase the risk of misuse but could rather improve biological security.

ACKNOWLEDGMENTS

A.N. was supported by a grant provided by the John D. and Catherine T. MacArthur Foundation.

1. Gibson, D.G. *et al. Science* **319**, 1215–1220 (2008).
2. Cello, J., Paul, A.V. & Wimmer, E. *Science* **297**, 1016–1018 (2002).
3. Tumpey, T.M. *et al. Science* **310**, 77–80 (2005).
4. Church, G. *Nature* **438**, 423 (2005).
5. Bugl, H. *et al. Nat. Biotechnol.* **25**, 627–629 (2007).
6. Garfinkel, M.S., Endy, D., Epstein, G.L., & Friedman, R.M. *Biosecur. Bioterror.* **5**, 59–62 (2007).
7. National Science Advisory Board for Biosecurity (NSABB). *Addressing Biosecurity Concerns Related to the Synthesis of Select Agents* (NSABB, Bethesda, Maryland, USA, 2006). http://oba.od.nih.gov/biosecurity/pdf/Final_NSABB_Report_on_Synthetic_Genomics.pdf
8. Tian, J. *et al. Nature* **432**, 1050–1054 (2004).
9. Kodumal, S.J. *et al. Proc. Natl. Acad. Sci. USA.* **101**, 15573–15578 (2004).
10. Kong, D.S., Carr, P.A., Chen, L., Zhang, S. & Jacobson, J.M. *Nucleic Acids Res.* **35**, e61 (2007).
11. International Atomic Energy Agency. *Annual Report 2006*, GC(51)/5 (International Atomic Energy Agency, Vienna, Austria, 2006). http://www.iaea.or.at/Publications/Reports/Anrep2006/anrep2006_full.pdf
12. Chyba, C.F. *Foreign Aff.* **81**, 122–136 (2002).
13. 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, USA, 2006).
14. Chyba, C.F. *Arms Control Today* **36**, 11–17 (2006).
15. Franco, C. *Biosecur. Bioterror.* **6**, 131–146 (2008).