Gene Synthesis

Methods and Protocols

Edited by

Jean Peccoud

Virginia Bioinformatics Institute, Virginia Tech, Blacksburg, VA, USA

Humana Press

Editor
Jean Peccoud, Ph.D.
Virginia Bioinformatics Institute
Virginia Tech
Blacksburg, VA, USA
jpeccoud@vbi.vt.edu

ISSN 1064-3745 e-ISSN 1940-6029

DOI 10.1007/978-1-61779-564-0
Springer New York Dordrecht Heidelberg London

Printed on acid-free paper

Humana Press is part of Springer Science+Business Media (www.springer.com/mycopy)

Preface

The de nov
significantly
manipulatin
However, ge
cells to mult
In this new
limiting step

Today, r
A variety of
enzyme-bas
DNAs that
tions. The
custom clon
reach a tacit
the cloning

Theore
transform sy
of any user-
sequences,
physical co
spend more
and less tim

One da
DNA fabric
tion period
complex pr
steps in att
have rushe
fabrication
commonly
ment. Dep
external ve
in house.
enabled by
skills. In an
(less than
raises a nur

Chapter 21

DNA Synthesis Security

Ali Nouri and Christopher F. Chyba

Abstract

It is generally assumed that genetic engineering advances will, inevitably, facilitate the misapplication of biotechnology toward the production of biological weapons. Unexpectedly, however, some of these very advances in the areas of DNA synthesis and sequencing may enable the implementation of automated and nonintrusive safeguards to avert the illicit applications of biotechnology. In the case of DNA synthesis, automated DNA screening tools could be built into DNA synthesizers in order to block the synthesis of hazardous agents. In addition, a comprehensive safety and security regime for dual-use genetic engineering research could include nonintrusive monitoring of DNA sequencing. This is increasingly feasible as laboratories outsource this service to just a few centralized sequencing factories. The adoption of automated, nonintrusive monitoring and surveillance of the DNA synthesis and sequencing pipelines may avert many risks associated with dual-use biotechnology. Here, we describe the historical background and current challenges associated with dual-use biotechnologies and propose strategies to address these challenges.

Key words: DNA engineering, DNA synthesis, Biosecurity, Biotechnology, Pathogen, Toxin

1. Introduction

The discovery of DNA structure by James Watson and Francis Crick (1), and Rosalind Franklin (2), and the subsequent elucidation of the genetic code at the Cavendish Laboratories (3) ultimately afforded scientists the ability to modify DNA and change the genetic makeup of living systems. Since then, areas of biotechnological power—in particular DNA sequencing and synthesis—have grown at a rapid pace. Some have compared such growth to "Moore's Law"—the exponential growth in computing power (4).

This growth in biotechnological power is coupled with the rapid diffusion of technologies. Just as Moore's Law led to a world of personal computers that are more powerful today than the most advanced computers were only decades ago, powerful biotechnologies are now increasingly accessible, affording to technically

Jean Peccoud (ed.), *Gene Synthesis: Methods and Protocols*, Methods in Molecular Biology, vol. 852,
DOI 10.1007/978-1-61779-564-0_21,

competent groups and even the individual user the sophisticated synthesis and manipulation of biological systems.

These advances have had a profoundly positive impact on human understanding of biological processes, and they have consequently improved health and well-being: genetically manipulating a cell's signal transduction pathway has led to the identification of drug targets, antibiotics, and other therapies; food security has been enhanced through the genetic modification of crops to produce varieties that are higher in yield than their wild-type counterparts or even ones that are resistant to disease and to drought; DNA manipulation has enabled the development of novel vaccines and rendered microbes that for centuries plagued humankind obsolete to the vaccinated.

But these same tools that have fundamentally improved human health and agriculture can also be used for ill: the same molecular biology methodologies that are employed to alter wild-type viruses into attenuated vaccine strains, for instance, could also be used to enhance their infectivity and pathogenicity for purposes of biological terrorism or warfare.

The challenge associated with biotechnology—and particularly with DNA synthesis technologies—is to ensure that they are only used for the advancement of humankind, rather than to its detriment. Striking this balance in a practical and efficient manner has thus far eluded policy makers because biotechnologies are extremely diffuse and exist in tens of thousands of academic and commercial laboratories worldwide (5).

Recent trends in the life sciences, however, lend themselves to the adoption of safeguards that were previously untenable. That is because biotechnology has become increasingly high-throughput and therefore increasingly automated. Automation of technologies such as DNA synthesizers and sequencers may enable the incorporation of automated safeguards either into machines or into a centralized clearinghouse to reduce the possibility of misusing such technologies for nefarious purposes (e.g., the creation of genetic material for bioterrorist purposes). During the development of novel technologies, there may be a small window of opportunity that scientists can capitalize upon in order to curb risks to ensure that their discipline is used only for legitimate purposes (6).

2. Dual-Use Biotechnology

The problem of biological weapons can be traced back centuries; whether it was catapulting bubonic plague-infested bodies over city walls by invading armies (7) or delivering smallpox virus-contaminated blankets to Native American tribes, humans resorted to biological warfare long before modern biology took hold.

With advances in biological research also came more advanced biological warfare programs. During WWII, for instance, the United States, United Kingdom, Soviet Union, and Germany all developed extensive chemical and biological warfare programs. These countries refrained from using them, but Japan attacked civilian populations extensively, including with fleas infected with *Yersinia pestis*—the causative agent of the bubonic plague (8). The US biological weapons program was ceased by executive order of President Richard Nixon. Subsequently, the Biological Weapons Convention—a multilateral treaty that prohibits the development, production, and stockpiling of biological weapons—was signed by the president and ratified by the US Senate. The Soviet Union, despite being a signatory to the treaty, continued a secret but elaborate and extensive offensive biological warfare program that apparently came to an end only with the disintegration of the USSR.

The ease with which biological organisms and toxins can be harnessed, amplified, and stockpiled has made them not just a threat that emanates from nation states but also from nonstate groups and even individuals. In 1984, the Rajneeshee, an Oregon-based cult, acquired Salmonella and contaminated restaurant salad bars, causing food poisoning in over 700 individuals. In 1995, the Japanese Aum Shinrikyo cult, which had previously attempted but failed in attacks on civilians with biological weapons, carried out attacks using the chemical weapon sarin, killing 13 and injuring dozens more in the Tokyo subway system. Many questions still remain with respect to the culprit behind the 2001 *Bacillus anthracis* "anthrax" attacks in the United States (9). Although he took his own life prior to the filing of formal charges by the FBI, that attack may have been carried out by Bruce Ivins, a biodefense researcher at the United States Army Medical Research Institute of Infectious Diseases. Even though the anthrax attacks resulted in only five deaths, they caused insecurity and substantial economic damage throughout the country (9).

One concern is that as biotechnologies diffuse throughout the world, and become increasingly user-friendly, the likelihood and potential damage of bioterrorism and biological warfare simply grow. There is already a list of well-known experiments that illustrate the capability and possible dangers intrinsic to biotechnologies, which are of dual-use: these technologies can be used for good or for ill. These experiments include genetic manipulation of mousepox—a cousin of smallpox—to the extent that the modified virus overcomes natural host immunity (10) (although humans are not susceptible to mousepox, the study's findings provide a potential blueprint to developing a vaccine-resistant smallpox virus); the creation of polio virus from scratch through the purchase of synthetic DNA molecules (11)—so that even if the World Health Organization (WHO) repeats its success with eradicating smallpox with that of eradicating polio worldwide, the virus could be created, de novo, in laboratories around the world; and the laboratory

resynthesis of the extinct Spanish influenza virus—the agent that killed tens of millions of people worldwide in the pandemic that began in 1918 (12). Although these experiments help elucidate the biology of disease-causing pathogens, the underlying tools—if misused—could result in catastrophic public health consequences. These dangers have been broadly recognized by committees of the US National Academies and the British Royal Society (5, 14, 15), but solutions that do not do more harm than good remain elusive. More recently, DNA synthesis capabilities integral to the emerging field of "synthetic biology," whose aims are to allow practitioners to fabricate small "biological devices" and ultimately new types of microbes (16) have further elevated previous security concerns. The synthesis of a 1.08-mega-base pair *Mycoplasma mycoides* genome and its transplantation into a *Mycoplasma capricolum* recipient cell to create new *M. mycoides* cells (17), for instance, raised concerns at the highest political levels and led President Obama to task his commission on bioethics to consider synthetic biology risks (18).

3. Challenges in Biological Security

Traditionally, there have been severe challenges to regulatory schemes that address risks for the field of biology (19) because (a) there is a mismatch between the rapid pace with which biotechnology advances, and the comparative sluggishness of creating and updating a regulatory regime; and (b) because monitoring and inspection of molecular biology laboratories is difficult, given that technologies are small scale and widespread. In the case of DNA synthesis technologies used for large, gene-length DNA synthesis, however, these challenges have been moderated in part because technologies are currently confined to relatively few facilities. This centralization makes a monitoring regime possible and has enabled much of the DNA synthesis industry to adopt safeguard strategies. Security concerns over this industry were heightened shortly after the technology was employed at the Stony Brook Laboratories in 2002 to synthesize the poliovirus DNA (11). To address risks associated with the fledgling field of DNA synthesis, Harvard biologist (and biotechnology developer and entrepreneur) George Church proposed a safeguard strategy to ensure that the technology will not be used for the illegitimate synthesis of potentially harmful genomes (20). In 2010, the National Institutes of Health published rules urging all companies engaged in large-molecule DNA synthesis to screen incoming requests for DNA above 200 nucleotides in length to ensure that sequences belonging to particular pathogens and

toxins are not commercially provided to certain individuals and states. Sequence comparison software is used to "read" DNA sequences of incoming customer orders and compare them to genes of toxins and genomes of a list of known pathogens, so that hazardous material is not produced for those that might have illicit intent (21).

The support of the synthesis industry for and adoption of these procedures is in part due to the nonintrusive nature of the proposal; rather than requiring oversight and cumbersome regulatory structures to which industry and many scientists might be opposed, the screening tool allows the DNA synthesis pipeline to go about business as usual while computer software engages in the invisible detective work. A major challenge going forward will be to harmonize the approach among all DNA providers worldwide since any noncompliant entity providing harmful material to unauthorized users undermines the framework. Possible strategies to address this deficiency include international guidelines, agreement, or even licensing for all DNA providers to follow a screening protocol, or establishing a centralized international clearinghouse that receives and screens all customer orders, clearing them for synthesis.

4. Synthesizer Proliferation and a New Security Paradigm

This risk-management framework embraced by industry may help prevent the misuse of commercially provided DNA molecules, but it will only be effective so long as the underlying tools remain confined to a relatively small number of facilities (22). Meanwhile, the increasing demand for synthetic DNA has made large-DNA synthesis lucrative, leading to the development of novel platforms that have potential for automation. One possible outcome could be the diffusion of advanced synthesizers—those capable of constructing large DNA molecules—to individual users around the world. Just as powerful computers once confined to the most advanced nations are now accessible to those who can afford them, one can envision a world in which graduate, undergraduate, perhaps even some high school biology students are provided with personal advanced DNA synthesizers as a standard laboratory bench-top research device. The diffusion of the polymerase chain reaction (PCR) machine to tens of thousands of laboratories worldwide demonstrates this possibility. This outcome would undermine, or even render irrelevant, the current risk-management framework adopted by the DNA synthesis industry. Therefore, alternative security strategies ought to be explored.

5. Conventional Biosecurity Strategies

Past attempts to safeguard the life sciences from misuse have proved challenging. This is because strategies that rely on restriction and classification of sensitive research, or on the curbing of scientific communication, limiting tacit knowledge, and restricting know-how, tend to be counterproductive for the life sciences, whose central mission is to improve human health and well-being. Life science research is the cornerstone of modern medicine. Despite its risks, for example, it is virology research that keeps lethal pathogens such as HIV at bay. And without information and material sharing regarding threatening pathogens such as methicilin-resistant *Staphylococcus aureus* (MRSA) and many others, there will be no treatment or cure. Any risk-management proposal that substantially hinders these medical-relevant efforts is and impractical—particularly given that life science research is already a thriving global endeavor.

The difficulty in devising concrete and unintrusive risk-management proposals for biotechnology has left the greater biology community with softer measures to guard against the possibility of misuse. Domestically, through the National Science Advisory Board for Biosecurity (NSABB), and internationally, through annual Biological Weapons Convention meetings, scientists, policy makers, and governments are largely relying on measures that include awareness-raising initiatives and ethics training as primary mechanisms by which biotechnology risks are addressed. Although these promote norms and encourage good behavior among well-intentioned individuals, they ought to be complemented with stronger measures that hinder the acquisition of biological material by those with illicit intent. Efforts to establish a monitoring regime for DNA synthesis companies represent an important approach. In addition, technologies, which are inherently resistant to being misused for illicit purposes, could further fill this gap.

6. Misuse-Resistant Technologies

As high-throughput large-scale research efforts gained traction in the life sciences, technologies that were only recently manual became increasingly automated. The absence of other measures, automation, and the consequent user-friendly nature of these technologies lowers the required expertise and increases the potential for these technologies to be misused for nefarious purposes. But if appropriately safeguarded, automation also provides opportunities to build safeguards into these technologies, so that only illicit applications are hindered. In the case of DNA synthesis, for

instance, safeguards could include built-in software or hardware that screens DNA sequence inputs and compares them to the sequences of pathogens and toxins of concern (22). Sequences could then be vetted as "legitimate" or "potentially nefarious."

An analogous concept is the so-called V-chip, a feature that can block the display of television programs of a particular rating. The V-chip is intended only to exert parental control over television viewing and can easily be reprogrammed; in the case of dual-use DNA synthesizers, such security measures would have to be more effective and robust.

For researchers registered to perform experiments with the genetic material of biological agents of concern, however, a software update or a modified computer chip permitting the user to bypass the synthesizer's restrictions could be utilized. Just as US regulations prohibit the transfer of hazardous biological agents to nonlicensed users, any software or hardware updates that permit bypassing of regulations would similarly only be available to appropriately vetted users. Of course, "hacking" these protections would have to be anticipated and countered.

Whereas these approaches would safeguard stand-alone synthesizers, alternatively, a "network security" approach could be employed, in which a central server that is in communication with remote synthesizers serves as the security focal point. Under this model, after users request DNA sequences online, the sequence filters through the server, which functions as a virtual DNA clearinghouse. Automated DNA screening at the server determines the identity of the DNA, as well as the identity of the user. While "legitimate" requests would simply filter through the clearinghouse and make their way to the user's synthesizer, any illegitimate order, such as a hazardous agent that is requested by an unauthorized user, would be terminated and the "job" transmitted to the appropriate national or international oversight agency.

One major challenge going forward is determining exactly what sequences would be regulated. Initially, a regulatory framework that already applies to the possession of pathogens and toxins of concern could be extended to their DNA sequences. In the USA, the possession of such "select agents" requires licensing by the Centers for Disease Control and Prevention or the Department of Agriculture. The Select Agent Regulations target the most dangerous pathogens. In order to minimize the regulatory burdens on biological research, these are currently limited to a small subset of dangerous organisms and toxins, despite the existence of numerous disease-causing agents that occur in nature. The National Academy of Sciences has now recommended that the extension of the select agent framework from biological agents to their genetic material be considered (23). This would facilitate the monitoring approaches the commercial DNA synthesis industry has adopted. Sequencing discrimination would be more challenging for genetic material that

is very similar, but not identical, to select agents. One can imagine, for instance, that an experienced researcher with illicit motives could simply request sequences that deviate from the original wild-type strain only slightly and yet still encode for pathogenic biologically active products. In the future, more comprehensive monitoring approaches will be needed to infer the pathogenicity of DNA sequences, despite human-induced changes in the sequence. More sophisticated approaches, however, such as the prediction of pathogenicity from novel sequences, are currently not available. Moreover, the Academies recently concluded that this approach is unlikely to be feasible for the purposes of a regulatory framework in the foreseeable future (23).

7. Oligonucleotide Synthesis

Thus far, concerns over DNA synthesis have involved only technologies that are capable of synthesizing large DNA molecules. Guidance from the National Institutes of Health, for instance, only urges companies to screen orders for DNA that are 200 nucleotides or longer. The majority of the synthetic DNA market, however, revolves around the production of oligonucleotides (oligos), which are DNA fragments that range from only a few to tens of nucleotides in length. Lack of a risk-management framework for this industry indeed enables a person to obtain a series of oligos that can be stitched together through standard biology techniques to make up longer genes.

Screening at the oligo level is challenging because such sequences are too small to provide "unique" features, making it impossible for sequence comparison software to assign a particular sequence to the organism of origin. If a number of these short sequences are pooled together, however, unique sequences could be revealed (Nouri, Goudarzi, and Chyba, unpublished). A security protocol for the oligonucleotide industry might be feasible if a centralized clearinghouse was established to pool a customer's disparate oligo requests—even if placed over separate time frames—so that the identity of the pooled sequences and thus the legitimacy of the order could be assessed.

Rather than providing a false sense of comfort by only safeguarding gene-size DNA manufacturers, a security framework that encompasses the much larger oligonucleotide industry ought to be explored.

8. Extending Screening from the DNA Synthesis to the DNA Sequencing Industry

While DNA screening at the synthesis bottleneck could be one effective tool for dealing with commercial DNA, it will not alleviate all biotechnology risks, which go well beyond DNA synthesis and include, for instance, genetic engineering experiments to enhance pathogens and toxins. We therefore set out to identify any bottlenecks associated with genetic engineering experiments that could be appropriately safeguarded. To uncover these, we analyzed scientific publications that utilize molecular biology and genetic engineering techniques and found that a necessary step in these experiments is DNA sequencing: almost invariably, researchers rely on DNA sequencing to gauge the success of molecular biology experiments such as constructing or altering a fragment of DNA or even the genome of an entire organism. Other potentially dual-use experiments, such as modifying hazardous bacterial and viral genomes, or construction of gene-encoding toxins, also require this verification step. The monitoring of the DNA sequencing phase of these experiments may provide clues as to the legitimacy of the underlying genetic engineering research and captures a host of potentially dangerous experiments that synthesis monitoring does not. While this proposal would have been much too intrusive and costly to implement in the days of manual DNA sequencing, advances in the field are opening new possibilities.

9. Outsourcing DNA Sequencing

DNA sequencing is among the fastest advancing biotechnologies; it used to be performed in-house using manual methodologies but is now increasingly automated. Centralized facilities that employ high-throughput technologies have sprung up to accommodate DNA sequencing needs of the life science community. This outsourcing is less error prone than traditional techniques and relieves researchers of the cumbersome task of manual sequencing. By 1999, 40% of US life science researchers engaged in DNA sequencing were outsourcing all sequencing work to only few facilities that served large numbers of users. By 2005, this figure had jumped to 80% (24). This centralization of DNA sequencing permits the adoption of monitoring and surveillance at these few locations. As customers submit DNA material for sequencing, samples can automatically be cross-referenced against the select agent database. Instances in which researchers who are not authorized to work with select agents submit select-agent DNA could result in the notification of appropriate authorities. This is similar to the screening

proposal already operating at some DNA synthesis factories where companies screen DNA orders to ensure that pathogenic genes and genomes are not provided to unauthorized customers. By adapting this protocol to the sequencing industry, a broad spectrum of risks that encompasses virtually all of recombinant DNA technologies could be partly mitigated.

Simultaneous with this outsourcing of DNA sequencing, however, there are major efforts on the part of the biotechnology industry to develop affordable, user-friendly, advanced personal sequencers. The diffusion of these to an increasing number of users would render a more centralized monitoring and surveillance strategy insufficient. To cope with this outcome, we also suggest that, in addition to the monitoring of centralized facilities, advanced personal DNA sequencers incorporate safeguards that recognize "illicit" sequences. Similar to the misuse-resistant synthesizers discussed above, sequencers could also be fitted with security software or built-in security chips that recognize select agent sequences and prohibit the sequencer from carrying out its function.

10. Paths Forward

Safeguarding the dual-use life sciences has been elusive, particularly because they are extremely widespread. Increasing automation in the synthesis and sequencing areas, however, provide opportunities to monitor DNA sequences and, thus, provide an opportunity to safeguard dual-use genetic engineering research. Those who wish to evade these safeguards could continue to perform in-house sequencing and synthesis using traditional (manual) tools. These methods, however, are more error prone, costly, and time-consuming, thereby reducing the likelihood and pace of success. Moreover, market forces will increasingly contribute to the eventual replacement of such manual technologies by advanced technologies amenable to safeguards. In any event, no safeguards regime can aspire to the total elimination of risk. The objective, rather, must be to mitigate risk without causing more harm than good.

These strategies can serve as focal points to safeguard the life sciences. The DNA synthesis industry has already begun implementing some of these approaches to deal with the narrow field of commercial DNA synthesis. If other biotechnology areas follow suit, a wide range of risks encompassing genetic engineering could be mitigated. Moreover, these preventative measures could be an important supplement to the current strategy of attempting to explore countermeasures against potential biological agents of concern.

Security strategies discussed above should be prioritized during early stages of technology development. Since the 2001

mail anthrax attacks, the federal government has spent over $50 billion just on civilian biodefense projects that include developing vaccines, drugs, and disease surveillance systems (25). In comparison, little attention is paid to developing biotechnologies and systems 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. If such technological-based security systems are prioritized, gradually improved automated technologies that are also safeguard-friendly will replace the older, less efficient, and difficult-to-safeguard tools.

Concurrent with the development of such technologies, it is also essential for a proper regulatory framework to be similarly advanced. As suggested by the Academies, this could include appropriate modification (26) and possible extension of rules that exist for the possession of particular organisms and toxins to their genetic sequences. For novel sequences, predicting pathogenicity based on sequence alone may not be possible in the foreseeable future, but better monitoring tools can be developed to detect select agent genome variants. Another important challenge will be to advance an international biotechnology security framework. Many countries lack national frameworks for dealing with the agents themselves, let alone their genetic material. And for those that have regulations in place, perceived biological threats vary greatly, leaving many hurdles to the creation of a harmonized global framework. The UN Secretary-General has recognized these challenges and called a global forum to address biotechnology risks. A methodical development of policies, nationally and internationally, together with the development and deployment of biotechnologies and bioservices that are intrinsically more secure will help ensure that the revolution in synthetic biology will only be used to benefit society.

References

1. Watson JD, Crick FH (1953) Molecular structure of nucleic acids; a structure for deoxyribose nucleic acid. Nature. 171:737–8.
2. Franklin RE and Gosling RG (1953) Molecular configuration in sodium thymonucleate. Nature 171, 740–741 (1953).
3. Crick FH, Barnett L, Brenner S, Watts-Tobin RJ (1961) General nature of the genetic code for proteins Nature 192:1227–32.
4. Moore, G (1965) Cramming More Components onto Integrated Circuits. Electronics pp114–7.
5. National Research Council (2006) 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. Washington, DC: National Academies Press.
6. Nouri A and Chyba CF (2008) Biotechnology and biosecurity. In: Bostrom N and Cirkovic MM (eds) Global Catastrophic Risks. Oxford University Press.
7. Wheelis, M (2002) Biological Warfare at the 1346 Siege of Caffa. Emerg Infect Dis 8:971–5.
8. Unit 731 Criminal Evidence Museum (2005). Unit 731: Japanese Germ Warfare Unit in China. China Intercontinental Press.

9. Shane S (2010). F.B.I., Laying Out Evidence, Closes Anthrax Case. The New York Times, February 19.
10. Jackson RJ et al (2001) Expression of mouse interleukin-4 by a recombinant ectromelia virus suppresses cytolytic lymphocyte responses and overcomes genetic resistance to mousepox. J Virol 75:1205–10.
11. Cello JP, Paul AV and Wimmer E (2002) Chemical synthesis of poliovirus cDNA: generation of infectious virus in the absence of natural template. Science 297:1016–8.
12. Tumpey TM et al (2005) Characterization of the reconstructed 1918 Spanish influenza pandemic virus. Science 310:77–80.
13. National Academy of Sciences (2003) Biotechnology research in an age of terrorism: Confronting the 'dual use' dilemma.5th ed National Academies Press, Washington DC.
14. 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.
15. The Royal Society (2009) New Approaches to Biological Risk Assessment. Royal Society Policy Document, United Kingdom.
16. Fu P (2006) A perspective of synthetic biology: Assembling building blocks for novel functions. Biotechnol J 1:690–9.
17. Gibson DG et al (2010) Creation of a bacterial cell controlled by a chemically synthesized genome. Science 329:52–6.
18. US President Obama's letter to his bioethics committee. www.bioethics.gov/documents/Letter-from-President-Obama-05.20.10.pdf.
19. Chyba CF. (2006) Biotechnology and the Challenge to Arms Control. Arms Control Today.http://www.armscontrol.org/act/2006_10/BioTechFeature.asp.
20. Church G (2005) Let us go forth and safely multiply Nature 438:423.
21. Bugl, H et al (2007) DNA synthesis and biological security Nat. Biotechnol 25:627–629 (2007).
22. Nouri A and Chyba CF (2009). Proliferation-resistant biotechnology: an approach to improve biological security. Nat Biotechnol 27: 234–236.
23. National Research Council (2010) Committee on Scientific Milestones for the Development of a Gene-Sequence-Based Classification System for the Oversight of Select Agents, Sequence-Based Classification of Select Agents: A Brighter Line. National Academies Press Washington, DC.
24. U.S. MSPPSA report on DNA Sequencing Market Analysis (2005/2006). http://www.phortech.com/2005seq.htm.
25. Franco C (2008). Billions for Biodefense. Biosecurity and Bioterrorism 6:131–146.
26. National Research Council (2009) Committee on Laboratory Security and Personnel Reliability Assurance Systems for Laboratories Conducting Research on Biological Select Agents and Toxins; Responsible Research with Select Agents and Toxins. National Academies Press Washington DC.