Lecture

Synthetic biology, security and governance

Filippa Lentzos

Department of Social Science, Health and Medicine, King's College London, Strand, London WC2R 2LS, UK.
E-mail: filippa.lentzos@kcl.ac.uk

Abstract The twenty-first century has witnessed an increasing confluence of rapidly advancing science and its embodiment in practical technologies, an extensive global diffusion of the knowledge and capabilities associated with those developments, and a seemingly unending shift in the international security environment. The scope and intensity of these interactions in the life sciences have generated concern about security risks stemming from possible misuse. This lecture focuses on one of the key emerging life science technologies of concern, gene synthesis, and considers how the new risks and challenges it poses for governance can best be managed.
BioSocieties (2012) **7,** 339–351. doi:10.1057/biosoc.2012.28; published online 26 November 2012

Keywords: gene synthesis; bioterrorism; biological weapons; risk; governance; regulation

Introduction

The regulation of unconventional weapons – chemical, biological, radiological and nuclear – has traditionally taken an 'artefact-centric' approach by seeking to control the materials, methods and products involved in misuse.[1] This approach is, however, particularly ill-suited to the life sciences, where the technologies are less about hardware, equipment and tools, and more about people, processes and know-how. Dual-use life science technologies are increasingly diffuse, globalized and multidisciplinary and are often based on intangible information rather than on specialized materials and equipment. This changes the definition of the problem from a material- and equipment-based threat that can be eliminated to a knowledge-based risk that must be managed. If what people know is more important than what people have, then the crucial factor becomes the choice that people will make about how they use the knowledge they have, and this changes fundamentally the kinds of measures to which policymakers must give attention (Moodie, 2012).

This lecture considers the emerging field of synthetic biology and focuses on one of its key enabling technologies: the ability to synthesize strands of DNA from off-the-shelf chemicals and assemble them into genes and microbial genomes. When combined with improved capabilities for the design and assembly of genetic circuits that perform specific tasks,

1 A version of this lecture was published by Filippa Lentzos and Pamela Silver (2012) 'Synthesis of viral genomes' in Jonathan Tucker (ed.) *Innovation, Dual-Use, and Security: Managing the Risk of Emerging Biological and Chemical Technologies*.

synthetic genomics has the potential for revolutionary advances. At the same time, it could permit the recreation of dangerous viruses from scratch, as well as genetic modifications designed to enhance the virulence and military utility of pathogens.

The potential misuse of gene synthesis to recreate deadly viruses for biological warfare or terrorism would require the integration of three processes: the automated synthesis of DNA segments, the assembly of those segments into a viral genome, and the production and weaponization of the synthetic virus. Each of these steps differs with respect to the maturity of the technologies involved, the ease with which it could be performed by non-experts and the associated threat. Even with access to synthetic DNA, assembling the DNA segments into a synthetic virus and converting the virus into a deliverable weapon would pose significant technical hurdles. This lecture reviews the security concerns related to DNA synthesis technology and advances a holistic governance approach, encompassing hard law, soft law and informal law, to limit the risk of misuse.

Overview of the Technology

The synthesis of viral genomes

DNA molecules consist of four fundamental building blocks: the nucleotide bases adenine (A), thymine (T), guanine (G) and cytosine (C), which can be linked together in any sequence to form a linear chain that encodes genetic information. A DNA molecule may consists of a single strand of nucleotide bases along a sugar backbone or two mirror-image strands that pair up to form a double helix, with adenine (A) always complementary to thymine (T) and guanine (G) complementary to cytosine (C). A second type of nucleic acid called RNA differs from DNA in the structure of its sugar backbone and the fact that one of the four nucleotide bases is uracil (U), which replaces thymine as the complementary base for adenine. An infectious virus consists of a long strand of single-stranded or double-stranded DNA or RNA, encased in a protein shell.

There are at least three ways to synthesize a viral genome *de novo* (from scratch). The first and most straightforward approach is to order the entire viral genome from a commercial gene-synthesis company by entering the DNA sequence on the company's Website. (A leading commercial supplier, Blue Heron Biotechnology in Bothell, WA, has synthesized DNA molecules up to 52 000 base pairs long.) The genomic sequence would be synthesized in a specialized facility using proprietary technology that is not available for purchase, packaged in a living bacterial cell and shipped back to the customer. The second option would be to order oligonucleotides (single-stranded DNA molecules <100 nucleotides in length) from one or more providers and then stitch them together in the correct order to create an entire viral genome. The advantage of this approach is that one can obtain more accurate DNA sequences, avoid purchasing expensive equipment and outsource the necessary technical expertise. The third option would be to synthesize oligonucleotides with a standard desktop DNA synthesizer and then assemble the short fragments into a genome. This approach would require acquiring a DNA synthesizer (purchased or custom-built) and a relatively small set of chemicals.

Although the chemical synthesis of oligonucleotides up to 120 base pairs is now routine, accurately synthesizing DNA sequences greater than 180 base pairs remains somewhat of an

art. For this reason, the *de novo* synthesis of most viruses is still more difficult than stealing a sample from a laboratory or isolating the agent from nature (Epstein, 2008). It is just a matter of time, however, before technological advances further reduce costs and the frequency of errors, making genome synthesis readily affordable and accessible (National Academies of Sciences, 2006).

A brief history of synthetic genomics

The field of synthetic genomics dates back to 1979, when the first gene was synthesized by chemical means (Khorana, 1979). The Indian-American chemist Har Gobind Khorana and 17 co-workers at the Massachusetts Institute of Technology took several years to produce a small gene made up of 207 DNA nucleotide base pairs. In the early 1980s, two technological developments facilitated the synthesis of DNA constructs: the invention of the automated DNA synthesizer and the polymerase chain reaction, which can copy any DNA sequence many million-fold. By the end of the 1980s, a DNA sequence of 2100 base pairs had been synthesized chemically (Mandecki *et al*, 1990).

In 2002, the first functional virus was synthesized from scratch: poliovirus, whose genome is a single-stranded RNA molecule about 7500 nucleotide base pairs long (Cello *et al*, 2002). Over a period of several months, Eckard Wimmer and his co-workers at the State University of New York at Stony Brook assembled the poliovirus genome from customized oligonucleotides, which they had ordered from a commercial supplier. When placed in a cell-free extract, the viral genome then directed the synthesis of infectious virus particles. The following year, Hamilton Smith and his colleagues at the J. Craig Venter Institute in Maryland published a description of the synthesis of a bacteriophage, a virus that infects bacteria, called φX174. Although this virus contains only 5386 DNA base pairs (fewer than poliovirus), the new technique greatly improved the speed of DNA synthesis. Compared with the more than a year that it took the Wimmer group to synthesize poliovirus, Smith and his colleagues made a precise, fully functional copy of the φX174 bacteriophage in only 2 weeks (Smith *et al*, 2003).

Since then, the pace of progress has been truly remarkable. In 2004, DNA sequences 14 600 and 32 000 nucleotides long were synthesized (Kodumai *et al*, 2004; Tian *et al*, 2004). In 2005, researchers at the US Centers for Disease Control and Prevention used sequence data derived from the frozen or paraffin-fixed cells of victims to reconstruct the genome of the 'Spanish' strain of influenza virus, which was responsible for the flu pandemic of 1918–1919 that killed tens of millions of people worldwide; the rationale for resurrecting this extinct virus was to gain insights into why it was so virulent. In late 2006, scientists resurrected a 'viral fossil', a human retrovirus that had been incorporated into the human genome around 5 million years ago (Enserink, 2006). In 2008, a bat virus related to the causative agent of human SARS was recreated in the laboratory (Skilton, 2008). That same year, the J. Craig Venter Institute synthesized an abridged version of the genome of the bacterium *Mycoplasma genitalium*, consisting of 583 000 DNA base pairs (Gibson *et al*, 2008). In May 2010, scientists at the Venter Institute announced the synthesis of the entire genome of the bacterium *Mycoplasma mycoides*, consisting of more than 1 million DNA base pairs (Gibson *et al*, 2010; Pennisi, 2010). The total synthesis of a bacterial genome from chemical building blocks was a major milestone in the use of DNA synthesis techniques to create more complex and functional products.

A methodological shift

Synthesizing a genome from scratch is a significant methodological shift from recombinant DNA technology, which involves the cutting and splicing of pre-existing genetic material. Because chemical synthesis can create any conceivable DNA sequence, it allows for greater efficiency and versatility in existing areas of research, while opening new paths of inquiry and innovation that were previously constrained.

Potential for Misuse

Only a few viral pathogens have any real military utility. Traditional effectiveness criteria for antipersonnel agents are infectivity (the ability to infect humans reliably and cause disease), virulence (the severity of the resulting illness), persistence (the length of time the pathogen remains infectious after being released into the environment) and stability when dispersed as an aerosol cloud. Early US developers of biological weapons preferred veterinary diseases such as anthrax, tularemia and Venezuelan equine encephalitis, which are not contagious in humans, because they made a biological attack more controllable. The Soviet Union, in contrast, weaponized contagious diseases such as pneumonic plague and smallpox for strategic attacks against distant targets, in the belief that the resulting epidemic would not boomerang against the Soviet population. The choice of pathogen also depends on the intended use, such as whether the aim is to kill or incapacitate, contaminate terrain for long periods or trigger a major epidemic.

Of the pathogenic viruses that can be found in nature, some are easier to isolate than others. Filoviruses such as Marburg and Ebola have animal reservoirs that are unknown, poorly understood or accessible only during active outbreaks. As a result, isolating these viruses from a natural source would require skill, good timing and the ability to transport the virus safely from the site of an outbreak. Because it is not easy to isolate natural strains with the desired characteristics, most pathogens developed in the past as biological weapons were either deliberately bred or genetically modified.

The increased accessibility and affordability of DNA synthesis techniques could eventually make it easier for would-be bioterrorists to acquire dangerous viral pathogens, particularly those that are restricted to a few high-security labs (such as the smallpox virus), are difficult to isolate from nature (such as Ebola and Marburg viruses) or have become extinct (such as the Spanish influenza virus). In theory, DNA synthesis techniques might also permit the creation of bioengineered agents more deadly and communicable than those that exist in nature, but in fact this scenario appears unlikely. As Tucker and Zilinskas (2006, p. 38) note:

> To create such an artificial pathogen, a capable synthetic biologist would need to assemble complexes of genes that, working in union, enable a microbe to infect a human host and cause illness and death. Designing the organism to be contagious, or capable of spreading from person to person, would be even more difficult. A synthetic pathogen would also have to be equipped with mechanisms to block the immunological defenses of the host, characteristics that natural pathogens have acquired over eons of evolution. Given these daunting technical obstacles, the threat of a synthetic 'super-pathogen' appears exaggerated, at least for the foreseeable future.

Accordingly, the most immediate risk of misuse associated with DNA synthesis technology is the recreation of known viral pathogens rather than the creation of entirely new ones. (As bacterial genomes are generally far larger than viral genomes, synthesizing them is more difficult and time-consuming.) Although the primary threat of misuse comes from state-level biological warfare programs, two possible scenarios involving individuals provide cause for concern. The first scenario involves a 'lone operator', such as a highly trained molecular biologist who is motivated to do harm by ideology or personal grievance. The second scenario involves a 'biohacker' who does not necessarily have malicious intent but seeks to create bioengineered organisms out of curiosity or to demonstrate technical prowess, a common motivation of many designers of computer viruses. As synthetic biology training becomes increasingly available to students at the college and even high-school levels, a 'hacker culture' may emerge, increasing the risk of reckless or malevolent experimentation (Tucker and Zilinskas, 2006, pp. 40–42).

Ease of misuse

In assessing the potential for misuse of DNA synthesis, it is important to examine the role of tacit knowledge in synthesizing a pathogen at the laboratory bench. The construction of a pathogenic virus by assembling pieces of synthetic DNA requires extensive training in basic molecular-biology techniques, such as ligation and cloning, including hands-on experience that is not 'reducible to recipes, equipment, and infrastructure' (Vogel, 2006, p. 676). This requirement for tacit knowledge is what the US National Science Advisory Board for Biosecurity (NSABB) meant when it noted that '[t]he technology for synthesizing DNA is readily accessible, straightforward and a fundamental tool used in current biological research. In contrast, the science of constructing and expressing viruses in the laboratory is more complex and somewhat of an art. It is the laboratory procedures downstream from the actual synthesis of DNA that are the limiting steps in recovering viruses from genetic material' (NSABB, 2006, p. 4).

The *World at Risk* report, released in December 2008 by the US Commission on the Prevention of WMD Proliferation and Terrorism, recommended that efforts to prevent bioterrorism focus less on the risk of terrorists becoming biologists and more on the risk of biologists becoming terrorists (WMD Commission, 2008). The report failed to emphasize, however, that not *all* biologists are of concern. Instead, the onus is on those who have worked in state-sponsored biological weapons programs and acquired both expertise and experience in weaponizing pathogens.

Accessibility of the technology

Synthesizing a virus and converting it into an effective biological weapon would require overcoming several technical hurdles. First, the *de novo* synthesis of an infectious viral genome requires an accurate genetic sequence. Although DNA or RNA sequences are available for many pathogenic viruses, the quality of the sequence data varies. Genomes published in publicly available databases often contain errors, some of which may be completely disabling whereas others would attenuate the virulence of a synthetic virus. In addition, some published sequences were not derived from natural viral strains but rather from cultures that had spent many generations in the lab and lost virulence through attenuating mutations.

A second difficulty with the synthesis of a highly pathogenic virus is ensuring infectivity. For some viruses, such as poliovirus, the genetic material is directly infectious, so introducing it into a susceptible cell results in the production of complete virus particles. For other viruses, such as causative agents of influenza and smallpox, the viral genome itself is not infectious and requires additional components (such as enzymes involved in replicating the genetic material) whose function must be replaced.

A third technical hurdle relates to the characteristics of the viral genome. Viruses with large genomes are harder to synthesize than those with small genomes. In addition, RNA viruses with one positive strand are easier to construct than RNA viruses with one negative strand, which in turn are easier to synthesize than double-stranded DNA viruses. Thus, poliovirus is relatively easy to synthesize because it has a small genome made of positive-stranded RNA, whereas the smallpox virus is hard to synthesize because it has a very large genome made up of double-stranded DNA. Synthesizing the Marburg and Ebola viruses would be moderately difficult: although their genomes are relatively small, they are not directly infectious and enabling them to produce virus particles would be challenging (WMD Commission, 2008). Despite these hurdles, the risk of misuse of DNA synthesis is expected to increase over time. One analyst has claimed that 10 years from now, it may be easier to synthesize almost any pathogenic virus than to obtain it by other means (WMD Commission, 2008, p. 15).

Nevertheless, even the successful synthesis of a virulent virus would not yield an effective biological weapon (Frerichs *et al*, 2004; Zilinskas, 2006). Once an appropriate viral pathogen has been synthesized, it would first have to be cultivated. Viruses are significantly harder to mass-produce than bacteria because they replicate only in living cells. One low-tech option would be to grow virus in fertilized eggs, but to avoid contamination the eggs would have to be specially ordered – not an easy task without attracting attention. Cultivating infectious virus is also extremely hazardous to the perpetrators and to those living nearby.

Disseminating biological agents effectively involves even greater technical hurdles. Whereas persistent chemical-warfare agents such as sulfur mustard and VX nerve gas are readily absorbed through the intact skin, bacteria and viruses cannot enter the body by that route unless the skin has been broken. Thus, biological agents must usually be ingested or inhaled to cause infection. To expose large numbers of people through the gastrointestinal tract, a possible means of delivery is the contamination of food or drinking water, yet neither of these scenarios would be easy to accomplish. Large urban reservoirs are usually unguarded, but unless the terrorists dumped in a massive quantity of biological agent, the dilution factor would be so great that no healthy person drinking the water would receive an infectious dose (Tucker, 2000). Moreover, modern sanitary techniques such as chlorination and filtration are designed to kill pathogens from natural sources and would probably be equally effective against a deliberately released agent.

The only way to inflict mass casualties with a biological agent is by disseminating it as an airborne aerosol: an invisible cloud of infectious droplets or particles so tiny that they remain suspended for long periods and can be inhaled by large numbers of people. A concentrated aerosol, released into the atmosphere of a densely populated urban area, could potentially infect many thousands of victims. After an incubation period of a few days (depending on the type of agent and the inhaled dose), the exposed population would experience an outbreak of incapacitating or fatal illness.

Nevertheless, the aerosol delivery of a biological agent entails major technical hurdles. To infect through the lungs, the infectious particles must be between 1 and 5 microns (millionths of a meter) in diameter. Generating an aerosol cloud with the particle size and concentration needed to cover a large area would require a sophisticated delivery system, such as an airborne sprayer. There is also a trade-off between the ease of production and the effectiveness of dissemination. The easiest way to produce microbial agents is in liquid form, yet when a slurry is sprayed into the air, it forms heavy droplets that fall to the ground so that only a small percentage of the agent is aerosolized. In contrast, if the microbes are dried to a solid cake and milled into a fine powder, they become far easier to aerosolize, but the drying and milling process is technically difficult.

Even if aerosolization could be achieved, the effective delivery of biological agents in the open air would depend on the prevailing atmospheric and wind conditions, creating additional uncertainties. Only under highly stable atmospheric conditions will an aerosol cloud remain close to the ground where it can be inhaled rather than being rapidly dispersed. Moreover, most microorganisms are sensitive to ultraviolet radiation and cannot survive more than 30 min in bright sunlight, limiting effective military use to nighttime attacks. The one major exception to this rule is anthrax bacteria, which can form spores with a tough protective coating that enables them to survive for several hours in sunlight. Terrorists could, of course, stage a biological attack inside an enclosed space such as a building, a subway station, a shopping mall or a sports arena, but even here the technical hurdles would be by no means trivial.

Finally, even if a synthetic virus was disseminated successfully in aerosol form, the outcome of the attack would depend on factors such as the basic health of the people who were exposed and the speed with which the public health authorities and medical professionals detected the outbreak and moved to contain it. A prompt response with effective medical countermeasures, such as the administration of antiviral drugs combined with vaccination, might significantly blunt the impact of an attack. In addition, simple, proven methods such as the isolation and home care of infected individuals, the wearing of face masks, frequent hand washing and the avoidance of hospitals where transmission rates are high have been effective at slowing the spread of epidemics. In sum, the technical challenges involved in carrying out a mass-casualty biological attack are formidable.

Imminence and magnitude of risk

Although the *de novo* synthesis of viral pathogens is relatively difficult today, rapid improvements in the cost, speed and accuracy of DNA synthesis mean that the risk of misuse of the technology will increase over time – although by how much remains a matter of debate. For the next 5 years, the greatest risk will involve the synthesis of a small number of highly pathogenic viruses that are currently extinct or otherwise difficult to obtain. Access to stocks of the smallpox virus and the Spanish influenza virus is tightly controlled: samples of the former are stored at two authorized repositories in the United States and Russia, while samples of the latter exist only in a few laboratories. Synthesizing the smallpox virus would be difficult because its genome is one of the largest of any virus and is not directly infectious. Although the genome of the 1918 influenza virus is relatively small and has been reconstructed and published, constructing the virus from scratch would be moderately difficult because the genome is not directly infectious (Garfinkel *et al*, 2007).

Contrary to worst-case planning scenarios, in which the aerosol dispersal of military-grade agents causes hundreds of thousands of deaths, only two bioterrorist attacks in the United States are known to have caused actual casualties. Both incidents involved the use of crude delivery methods: the deliberate contamination of food with *Salmonella* bacteria by the Rajneeshee cult in Oregon in 1984, and the mailing of powdered anthrax spores through the postal system in 2001. Such low-tech attacks are likely to remain the most common form of bioterrorism. They are potentially capable of inflicting at most tens to hundreds of fatalities – within the destructive range of high-explosive bombs, but not the mass death predicted by many worst-case scenarios (Tucker, 2000).

Oversight

Current governance measures

Much can be done at the national or regional level to manage the risk of misuse of DNA synthesis. The fact that only about 50 companies worldwide currently possess the advanced know-how and technical infrastructure needed to produce gene-length DNA molecules offers a window of opportunity to introduce governance measures.

In Europe, concerns about genome synthesis have focused on biosafety, the nature and integrity of life, equity and intellectual property, and public confidence and engagement, rather than on security and deliberate misuse (Schmidt, 2006; Feakes, 2008/2009; Lentzos, 2009). Typical of this approach is the European Commission's assessment that the most pressing need is 'to examine whether existing safety regulations for the management of engineered microorganisms provide adequate protection against inadvertent release of "synthetic" pathogens. In particular, who is responsible for ascertaining and quantifying risks, and for implementing any clean-up measures that might be undertaken?' (European Commission, 2005). Two European countries, the United Kingdom and the Netherlands, stand out as having considered the biosecurity aspects of synthetic genomics in some detail, and both have concluded that the current regulatory frameworks are adequate to address the risk of misuse.

The United States has been far more aggressive in addressing the security dimensions of gene synthesis. In November 2009, the Department of Health and Human Services (DHHS) published a draft 'Screening Framework Guidance for Synthetic Double-Stranded DNA Providers' in the *Federal Register*, and the finalized guidelines were published a year later, in October 2010 (US DHHS, 2009). These guidelines call for subjecting all requests for synthetic double-stranded DNA to a process of customer and sequence screening. Upon receiving a DNA synthesis order, the supplier should review the information provided by the customer to verify its accuracy and check for 'red flags' suggestive of illicit activity. If the information provided raises concerns, the supplier should ask the customer for additional information. Screening the requested DNA sequence to identify any sequences derived from or encoding Select Agents is also recommended. If the customer or the sequence raises concerns, providers are urged to clarify the intended end-use. In cases where follow-up screening does not resolve the concern, providers are encouraged to seek advice from designated government officials. The US guidance document also recommends that providers retain electronic copies of customer orders for at least 8 years, the duration of the statute of limitations for prosecution. Although adherence to the screening framework is considered voluntary, the guidance reminds providers of their legal obligations under existing export control regulations.

Recognizing the security concerns associated with synthetic DNA, a number of gene-synthesis companies have already begun screening customers and orders on their own initiative (International Association of Synthetic Biology (IASB), 2008). The IASB, a consortium of mainly German companies, launched its 'Code of Conduct for Best Practices in Gene Synthesis' on 3 November 2009 (Lok, 2009). Like the US government guidance document, the Code of Conduct recommends an initial screen to confirm the customer's *bona fides*, followed by an automated screen of the sequence order using a computer program to search for similarities between gene sequences. Any hits from the automated screen are then assessed by human experts. If the hits are judged to be real and not false-positives, follow-up screening is done to verify the legitimacy of the customer before the order is filled (IASB, 2008). Shortly before the IASB Code of Conduct was launched, two companies that had initially been involved in the process dropped out and established their own group, the International Gene Synthesis Consortium (IGSC). This body includes five of the world's leading gene-synthesis companies and claims to represent 80 per cent of the industry (Check Hayden, 2009). Because of its large market share, the IGSC asserts it has the experience to develop workable screening measures and has put forward a 'Harmonized Screening Protocol' to rival the IASB Code of Conduct (Bhattacharjee, 2009). As a result, gene-synthesis companies have been left to decide whether to adopt one of the three competing standards, to devise their own by mixing and matching various elements or to ignore the process altogether.

A new governance framework

Previous surveys on the effectiveness of voluntary self-governance in the biotechnology industry have highlighted inconsistencies in the way the regimes are implemented (Lentzos, 2006). For example, biotechnology companies vary greatly in how they use Institutional Biosafety Committees (IBCs) to review recombinant-DNA research, including the structure of the committees, the frequency of meetings, the quality of minutes produced, and whether or not the committees approve individual projects or groups of projects. The IBCs also differ in how they interpret their purpose and responsibilities (Lentzos, 2006). Similarly, most providers of synthetic DNA are sensitive to security concerns and would probably agree to implement some sort of screening practices if they are not doing so already, but it is unclear what the minimum standards should be. Who decides if the DNA sequence database used for screening purposes is adequate? Is it sufficient to retain order records in the form of broad statistics, or must the details of each individual order be kept? Is 5 years long enough to retain records, rather than 8? One way to settle such questions is to establish a set of minimum screening standards through statutory legislation rather than voluntary guidance.

In devising a governance framework for the *de novo* synthesis of viral genomes, it is useful to think of regulation as a process that operates through three different mechanisms to influence both formal and informal behavior (Corneliussen, 2001; Lentzos, 2008). 'Hard law' regulates companies by explicitly imposing certain practices through statutory legislation, 'soft law' regulates companies by standardizing particular practices and 'informal law' regulates companies by designating particular practices as necessary for success. Compliance with the three forms of regulation confers organizational legitimacy on companies and helps to ensure their survival. The most effective regulatory frameworks include all three kinds of law reinforcing each other.

Much of the discussion on the regulation of gene synthesis has focused on ensuring that the burgeoning gene-synthesis industry does not bear unnecessary burdens. Yet regulatory law can benefit suppliers if it increases public confidence in the technology. This advantage is particularly relevant in the biotechnology field because private biotech companies ultimately depend on social support for the creation of new markets. Moreover, a regulatory regime that leads companies to act in a responsible manner (and to be seen as doing so) may actually be more profitable than a less restrictive regime that generates constant controversy and hostile campaigning. Indeed, Michael Porter has argued that strict environmental regulations, rather than shifting external costs onto companies and burdening them relative to competitors in countries with less stringent regulations, can result in a 'win-win' situation in which the companies' private costs are reduced along with the external costs they impose on the environment (Porter and van der Linde, 1995). Porter concludes, 'Strict environmental regulations do not inevitably hinder competitive advantage against foreign rivals, indeed, they often enhance it'. Thus, the synthetic DNA industry could potentially benefit from a regulatory regime that carefully balances stringency with legitimacy, although this solution would require companies to accept a certain regulatory burden.

Arguing for statutory legislation is not meant to imply that voluntary measures have no merit. Self-governance may provide incentives for companies to behave in a responsible way. The reward for adopting screening practices, for example, is inclusion in the 'club' of companies that are seen as reputable and 'doing the right thing', sending a positive signal to customers and investors. In this way, successful companies can help to regulate others by designating screening practices as necessary for economic success. If, however, the screening guidelines are not generally adhered to, then self-governance may discourage other companies from implementing them, especially when there are costs involved. This is a situation where the force of law can be particularly persuasive. Indeed, the gene-synthesis industry has recognized the problem of non-compliance with voluntary guidelines. A workshop report from the IASB notes, 'Ultimately, the definition of standards and the enforcement of compliance with these is a government task' (IASB, 2008, p. 14).

Statutory legislation is also important for managing rogue companies. Commenting on the IASB's early efforts to develop a code of conduct, a *Nature* Editorial argued that they were 'laudable first steps' but that synthetic DNA providers 'still need independent oversight' in the form of statutory legislation.

> There have been, and will probably continue to be, companies that are not interested in cooperating with any industry group, and that are happy to operate in the unregulated grey area. The ultimate hope is that customers will put economic pressure on those non-compliers to fall in line, or else lose all but the most disreputable business. But that is just a hope. As the recent meltdowns on Wall Street have indicated, industry self-policing can sometimes fail dramatically. When bad business practices can have grave effects for the public, regulators should be firm and proactive. (*Nature* Editorial, 2008)

Another approach is professionalization, which lies between self-governance and statutory measures. In most jurisdictions, all professional practitioners are licensed and belong to an association established by law, which sets the standards of practice for its members in order

to align them with the public good. The officers of the association are elected by the members and are expected to be advocates for the profession. This combination of a legislated mandate and collegial self-governance provides accountability for the profession as a whole and for its individual practitioners. Weir and Selgelid argue that the professionalization of synthetic biology would establish educational standards for its members and define normative standards of practice, with the aim of ensuring competence and preventing misconduct. By combining self-governance and legally-authorized governance, this approach avoids the polarization that has characterized much of the debate over the regulation of synthetic biology (Weir and Selgelid, 2009).

Conclusion

DNA synthesis is a powerful enabling technology that has many beneficial applications but also entails a significant risk of misuse. An optimal strategy to limit this risk would entail applying the three modes of governance (hard law, soft law and informal law) to DNA synthesis so that (i) national governments regulate companies by imposing a baseline of minimum security measures that all providers of synthetic DNA must adopt; (ii) the DNA synthesis community reinforces the statutory legislation through a professional code of conduct that regulates gene-synthesis companies across borders and encourages universal adherence despite differing national assessments of the risk of misuse; and (iii) role-model companies, such as commercial suppliers that have adopted the IASB or IGSC protocols, regulate other companies by designating screening practices as necessary for economic success, much as ISO accreditation and other non-statutory regimes have become accepted as requirements to operate in other fields.

About the Author

Filippa Lentzos is a Senior Research Fellow in the Department of Social Science, Health and Medicine at King's College London. Her primary research interests are focused on biosecurity and synthetic biology, and the range of social, ethical, political, legal, economic and geographical issues associated with these two key emerging research themes in the field of biomedicine and society. She is especially interested in the social shaping of risks and threats, and in the social organization and deployment of evidence, facts and knowledge. Her current research on the politics of bioterrorism is funded by an ESRC Mid-Career Fellowship.

References

Bhattacharjee, J. (2009) Gene synthesis companies pledge to foil Bioterrorists. *Science*, http://news.sciencemag.org/scienceinsider/2009/11/gene-synthesis.html, accessed 11 October 2012.

Cello, J., Paul, A.V. and Wimmer, E. (2002) Chemical synthesis of poliovirus cDNA: Generation of infectious virus in the absence of natural template. *Science* 297(5583): 1016–1018.

Check Hayden, E. (2009) Gene-makers form security coalition. *Nature*, http://www.nature.com/news/2009/091118/full/news.2009.1095.html, accessed 11 October 2012.

Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism (WMD Commission). (2008) *World at Risk*. New York: Vintage Books.

Corneliussen, F. (2001) The legal trichotomy: Biotech company perspectives on institutional elements constraining research activities. *Zeitschrift für Rechtssoziologie* 22(2): 1–18.

Enserink, M. (2006) Viral fossil brought back to life. *Science Now*, http://news.sciencemag.org/sciencenow/2006/11/01-04.html, accessed 11 October 2012.

Epstein, G. (2008) The challenges of developing synthetic pathogens. *Bulletin of the Atomic Scientists*, 19 May, http://www.thebulletin.org/web-edition/features/the-challenges-of-developing-synthetic-pathogens, accessed 11 October 2012.

European Commission. (2005) Synthetic Biology: Applying Engineering to Biology. Brussels: Directorate General Research. Report of a NEST High-Level Expert Group.

Feakes, D. (December 2008/January 2009) Synthetic biology and security: A European perspective. *WMD Insights* 29: 15–24.

Frerichs, R.L. *et al* (2004) *Historical Precedence and Technical Requirements of Biological Weapons Use: A Threat Assessment*, SAND2004-1854, Albuquerque, NM: Sandia National Laboratories.

Garfinkel, M.S., Endy, D., Epstein, G.L. and Friedman, R.M. (2007) *Synthetic Genomics: Options for Governance*. Rockville, MD: J. Craig Venter Institute, pp. 13–14.

Gibson, D.G. *et al* (2008) Complete chemical synthesis, assembly, and cloning of *Mycoplasma genitalium* Genome. *Science* 319(5867): 1215–1220.

Gibson, D.G. *et al* (2010) Creation of a bacterial cell controlled by a chemically synthesized genome. *Science* 329(5987): 52–56.

Industry Association Synthetic Biology (IASB). (2008) Report on the Workshop 'Technical Solutions for Biosecurity in Synthetic Biology'. 3 April, Munich, Germany, http://www.synbiosafe.eu/uploads///pdf/iasb_report_biosecurity_syntheticbiology.pdf, accessed 11 October 2012.

Khorana, H.G. (1979) Total synthesis of a gene. *Science* 203(4381): 614–625.

Kodumai, S.J., Patel, K.G., Reid, R., Menzella, H.G., Welch, M. and Santi, D.V. (2004) Total synthesis of long DNA sequences: Synthesis of a contagious 32-kb Polyketide Synthase gene cluster. *Proceedings of the National Academy of Sciences* 101(44): 15573–15578.

Lentzos, F. (2006) Managing biorisks: Considering codes of conduct. *Nonproliferation Review* 13(2): 211–226.

Lentzos, F. (2008) Countering misuse of life sciences through regulatory multiplicity. *Science and Public Policy* 35(1): 55–64.

Lentzos, F. (2009) Synthetic biology in the social context: The UK debate to date. *BioSocieties* 4(3–4): 303–315.

Lentzos, F. and Silver, P. (2012) Synthesis of viral genomes. In: J. Tucker (ed.) *Innovation, Dual-Use, and Security: Managing the Risk of Emerging Biological and Chemical Technologies*. Cambridge, MA: MIT Press.

Lok, C. (2009) Gene-makers put forward security standards. *Nature*, http://www.nature.com/news/2009/091104/full/news.2009.1065.html, accessed 11 October 2012.

Mandecki, W., Hayden, M.A., Shallcross, M.A. and Stotland, E. (1990) A totally synthetic plasmid for general cloning, gene expression and mutagenesis in *Escherichia coli*. *Gene* 94(1): 103–107.

Moodie, M. (2012) Managing the security risks of emerging technologies. *Arms Control Today* 42(September).

National Academies of Sciences. (2006) *Globalization, Biosecurity, and the Future of the Life Sciences*. Washington DC: National Academies of Sciences.

National Science Advisory Board for Biosecurity (NSABB). (2006) *Addressing Biosecurity Concerns Related to the Synthesis of Select Agents*. Bethesda, MD: National Institutes of Health.

Nature Editorial. (2008) Pathways to security. *Nature* 455(7212): 432.

Pennisi, E. (2010) Synthetic genome brings new life to bacterium. *Science* 328(5981): 958–959.

Porter, M.E. and van der Linde, C. (1995) Green and competitive: Ending the stalemate. *Harvard Business Review* 73(5): 120–134.

Schmidt, M. (2006) Public will fear biological accidents, not just attacks. *Nature* 441(7097): 1048.

Skilton, N. (2008) Man-made SARS virus spreads fear. *Canberra Times*, 24 December.

Smith, H.O., Hutchinson III, C.A., Pfannkoch, C. and Venter, J.C. (2003) Generating a synthetic genome by whole genome assembly: φX174 Bacteriophage from synthetic oligonucleotides. *Proceedings of the National Academy of Sciences* 100(26): 15440–15445.

Tian, J. *et al* (2004) Accurate multiplex gene synthesis from programmable DNA microchips. *Nature* 432(7020): 1050–1054.

Tucker, J.B. (2000) Introduction. In: J.B. Tucker (ed.) *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*. Cambridge, MA: MIT Press, pp. 1–14.

Tucker, J.B. and Zilinskas, R.A (2006) The promise and perils of synthetic biology. *The New Atlantis* 25(12): 25–45.

US Department of Health and Human Services (DHHS). (2009) Screening framework guidance for synthetic double-stranded DNA providers. *Federal Register* 74(227): 62319–62327.

Vogel, K. (2006) Bioweapons proliferation: Where science studies and public policy collide. *Social Studies of Science* 36(5): 659–690.

Weir, L. and Selgelid, M.J. (2009) Professionalization as a governance strategy for synthetic biology. *Systems and Synthetic Biology* 3(1–4): 91–97.

Zilinskas, R.A. (2006) Appendix C: Technical barriers to successful biological attacks with synthetic organisms. In: S.M. Mauer, K.V. Lucas and S. Terrell (eds.) *From Understanding to Action: Community-Based Option for Improving Safety and Security in Synthetic Biology.* Berkeley, CA: University of California, p. 8.