

MIT Open Access Articles

What rough beast? Synthetic Biology and the Future of Biosecurity

The MIT Faculty has made this article openly available. **Please share** how this access benefits you. Your story matters.

Citation: Mukunda, Gautam, Kenneth A. Oye, and Scott C. Mohr. "What Rough Beast?" *Politics and the Life Sciences* 28.2 (2009): 2–26. Web. 30 Mar. 2012.

As Published: http://dx.doi.org/10.2990/28_2_2

Publisher: BioOne (Politics and the Life Sciences)

Persistent URL: <http://hdl.handle.net/1721.1/69908>

Version: Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

Terms of use: Creative Commons Attribution-Noncommercial-Share Alike 3.0



WHAT ROUGH BEAST?

SYNTHETIC BIOLOGY, UNCERTAINTY, AND THE FUTURE OF BIOSECURITY

Gautam Mukunda, Department of Political Science, MIT
Kenneth A. Oye, Engineering Systems Division and Department of Political Science,
MIT
Scott C. Mohr, Department of Chemistry, Boston University

August 2009

“A shape with lion body and the head of a man,
/.../
And what rough beast, its hour come round at last,

Slouches towards Bethlehem to be born?”

William Butler Yeats: *The Second Coming*

Abstract

Synthetic biology (SB) seeks to create modular biological parts that can be assembled into useful devices, allowing the modification of biological systems with greater reliability, at lower cost, with greater speed, and by a larger pool of people than has been the case with traditional genetic engineering. We assess the offensive and defensive security implications of SB based on the insights of leading synthetic biologists into how the technology may develop, the projections of practicing biosecurity authorities on changes in security context and on potential security applications of SB, and joint appraisals of policy-relevant sources of uncertainty. SB appears to have minimal security implications in the near term, to create modest offensive advantages in the medium term, and to strengthen defensive capabilities against natural and engineered biological threats and to enable novel potential offensive uses in the long term. To maximize defensive and minimize offensive effects of SB despite uncertainty, this essay suggests a combination of policy approaches including community-based efforts, regulation and surveillance, further research, and the deliberate design of security and safety into the technology.

Keywords: Synthetic Biology; Biosecurity; Biodefense; Biological Weapons

Introduction

After decades without significant use of biological weapons, official concerns over the possibility of a biological attack are rising. There have been no verified instances of any state using biological weapons since World War II. The United States and Soviet Union researched and produced biological weapons, but never used the weapons they stockpiled. Non-state actors have used biological weapons, but have had little success when doing so. Two religious cults attempted to cause mass casualties using biological weapons, but no deaths resulted from their attacks. Soon after the September 11th attacks, however, a series of anthrax attacks by a rogue scientist from a U.S. weapons laboratory resulted in 5 fatalities and 17 infections.^{1,2,3,4} This incident, combined with continuing advances in humanity's ability to manipulate living systems, has motivated official and unofficial reassessments of the threat from biological weapons, particularly in the hands of non-state actors.

The Central Intelligence Agency (CIA) Office of Transnational Issues (2003), the National Research Council (2004) and the National Science Advisory Board Recombinant DNA Advisory Committee (NSABB/RAC) (2007) are among many organizations directing attention to what they see as a growing security threat. Nongovernmental organizations, science reporters, and science fiction writers have echoed these official concerns.^{5,6,7} Most recently, the U.S. Commission on Prevention of WMD Proliferation and Terrorism – usually called the Graham-Talent Commission after its Chair and Vice-Chair - issued a report titled “World at Risk” (2008). The Commission concluded that it is more likely than not that a terrorist attack using a weapon of mass destruction will occur somewhere in the world by the end of 2013, and concluded that “terrorists are more likely to be able to obtain and use a biological weapon than a nuclear weapon.” There thus exists a broad consensus that progress in biotechnology is likely to increase the danger from biological weapons, even as there exists heated debate on the current level of threat they present.^{8,9,10,11,12,13,14,15,16,17,18}

These analysts suggest that rapid progress in the life sciences, particularly genetic engineering, means that the future of biological warfare may not look like the past. Two developments in particular have been the foci of attention. First, the basic tools of biological engineering have been developing rapidly, with exponential advances in productivity and declines in cost of DNA synthesis. The security implications of DNA synthesis are already matters of concern and have been extensively studied.^{19,20} Second, biological engineers known as Synthetic Biologists are using these tools to develop modularized approaches to the design and recombination of genetic materials. Practitioners of Synthetic Biology (SB) aspire to make genetic engineering easier, cheaper, more efficient, and more predictable, thereby accelerating the advance of biotechnology. If successful, SB will also allow many more people to engage in the redesign of biological components and systems. At present, the aspirations of Synthetic Biologists remain largely unfulfilled. Yet even at this relatively early stage of development, concerns over the security implications of DNA synthesis and Synthetic Biology are driven by a belief that their continued advancement will improve the effectiveness of biological weapons while reducing impediments to their acquisition and utilization by state and non-state actors alike.²¹

Are these concerns well-founded? This essay analyzes the marginal effects of further improvements in DNA synthesis and SB on both defensive and offensive capabilities and recommends policies that may mitigate some of the security concerns which may arise. The study is based on anonymous interviews with the most widely-published and frequently-cited practitioners of SB and nationally-recognized authorities on biosecurity, reviews of the literature on the production and use of biological weapons, and independent analysis by the authors. Forecasting is, at best, a difficult task, and the record of forecasting in science and technology policy is particularly dismal.^{22,23} With this in mind, the essay also seeks to characterize uncertainty associated with the development and application of SB and discuss ways that uncertainty may be addressed more effectively in policy.

This paper is organized into seven sections. First is a description of this study's methodology. Second is a primer for non-biologists on the essentials of SB, with a discussion of how that emerging field

differs from conventional genetic engineering. Third is an evaluation of the contribution of SB to weapons production and a brief discussion of weapons development processes, with illustrations of how existing benign contributions from SB might be used in developing biological weapons. Fourth is an examination of how SB techniques may affect defensive capabilities against both natural epidemics and artificial threats, with attention to enhanced surveillance for bioweapons, accelerated vaccine development, and development of advanced therapies. Also included is a projection of how the balance between offensive and defensive biological capabilities may shift over time. Fifth is an analysis of how SB's focus on decreasing the skill necessary to modify biological systems and its emphasis on modularity of design may have security implications substantially beyond those normally attributed to advances in biotechnology. Sixth is a set of policy recommendations on how governments and the research community should minimize the dangers and maximize the benefits from the progress of biotechnology. Seventh is a summary of key conclusions on near term, medium term, and long term security implications of SB on offensive and defensive capabilities and recommendations for designing policies that engage with uncertainty over these effects.

Methodology

Our research was conducted in four stages. First, we began with a review of the extant literature on biosecurity, focusing on earlier work on the implications of technological change on biosecurity. We used this review of the literature to develop a detailed interview guide for use in a series of comprehensive interviews with nationally-recognized leaders in Synthetic Biology and biosecurity. Second, we selected interview subjects based on expertise in relevant fields, interest in issues involving the nexus between SB and biosecurity, and willingness to engage in a time-consuming interview process. We conducted eight such initial interviews, which averaged approximately one-and-a-half hours in length. The interview subjects are described in Table 1. All interview subjects were promised anonymity to

assure their complete freedom to answer questions on a highly controversial topic like biosecurity. Based on these interviews we formulated tentative initial conclusions and policy recommendations. Third, we checked our initial conclusions with our original interview subjects and a wide variety of other people with expertise in SB and/or biosecurity. We did this by conducting more narrowly focused interviews with more than 30 people with particular knowledge of aspects of SB and biosecurity and by convening small group discussions on specific topics and policy recommendations. We then revised our conclusions and analysis based on this second round of interviews, which averaged one hour in length for one-on-one interviews and two or more hours for the small group discussions. Finally, we secured additional feedback on preliminary versions of our analysis and conclusions, presenting them to approximately 1000 people in a variety of settings, including the 2007 Synthetic Biology 3.0 in Zurich and the 2009 American Society of Microbiologists Biodefense Meeting, and meeting with many audience members both informally and in formal interviews after every presentation.

Such an iterated interview based research design had several advantages. It allowed us to capture a broad spectrum of views in both the Synthetic Biology and biosecurity communities, both within and beyond the United States. It allowed us to highlight key areas of disagreement and controversy within the Synthetic Biology and biosecurity communities by providing repeated in-depth discussions over prolonged periods of time with actors with a wide array of perspectives on the situations. Finally, and most importantly, it allowed us to incorporate the ideas and views of people with a wide variety of perspectives on key issues and points of disagreement. This series of interviews allowed key topics, ideas, and concepts to be rapidly identified then discussed and analyzed in depth, with information, predictions, and conclusions subject to detailed reexamination and discussion.

What is Synthetic Biology?

Altering the DNA of natural evolved systems to serve human ends is inherently difficult. Because even the simplest bacterium has an evolutionary heritage stretching back billions of years, natural biological systems are highly complex and tightly integrated with other biological systems. These natural systems are thus usually only partially understood, which makes modifying them exceptionally difficult. When attempting to do so, failures are both frequent and inevitable. Every interview subject with experience as a bioengineer described traditional genetic engineering as a craft, with one-off customized development of biological devices done by highly skilled technologists.²⁴ Synthetic Biology seeks to turn biological engineering into an industrial process by developing modularized genetic parts that may be reused and assembled into useful biological devices by less skilled technologists. SB shares with traditional genetic engineering the goal of developing practical applications ranging from the biosynthesis of pharmaceuticals, polymers, and fuels, the detection and measurement of pollutants, drugs, and tumors, and the creation of controls that respond to light, temperature and other signals. SB differs from traditional genetic engineering, however, in its emphasis on developing modularized biological parts, protocols for interoperability and standards for parts performance, open parts registries to foster use by all, and routinized methods of assembly for creating biological devices.^{25,26}

This brief primer on SB proceeds through three stages. First, it describes how DNA sequencing and systems biology provided the information that is now the foundation for SB. Second, it reviews briefly how principles of modularity and standardized assembly evolved, beginning with assembly of the “repressilator” from components to formalization of the principle of idempotent assembly to formation of registries of standardized parts. Third, it discusses briefly how the application of principles of modular design may cut design costs and development times, allow parts outsourcing with resulting scale economies, and allow more rapid diffusion of the methods of biological design.

Foundations of Synthetic Biology: Genomic Data and Systems Biology

Synthetic Biology is founded in the transformation of biology brought about by our ability to determine the complete sequences of the DNA molecules that constitute an organism's genome. DNA encodes genetic information in a linear string of molecular groups called "bases" symbolized by the initials of their chemical names A, C, G and T. Determination of the precise sequence of these groups establishes nearly all of an organism's hereditary information. Some hereditary information is not carried in DNA, however, and may need to be understood and accounted for when Synthetic Biologists begin to modify cellular machinery more substantially than they have so far.

Whole-genome sequencing began with small viruses in the 1970s, but the first cellular genome from a living organism, the bacterium *Haemophilus influenzae*, was not completely sequenced until 1995. Larger genomes were soon sequenced, including those of bakers' yeast, a nematode worm, the common fruit fly and, by 2000, human beings. By mid-2008, complete genomes were available for 931 prokaryotes (microorganisms that lack nuclei) and 24 eukaryotes (organisms with nucleated cells, including humans). An additional 557 eukaryotic genome sequences are in varying stages of completion.^{27,28}

All of these sequenced genomes are available in the public domain on the internet through GenBank (USA), EMBL (Britain), and DDBJ (Japan), which share and exchange sequence information on a daily basis. These genomes plus additional genetic information from other species represent a treasure trove of biological functions evolved during the more than 3.8 billion years since life on Earth began – a smorgasbord as it were, that invites experimentation and exploitation. Figure 1 shows the dramatic growth of the public genome database over the past 15 years. It now contains nearly 100 trillion letters of the genetic alphabet.²⁹

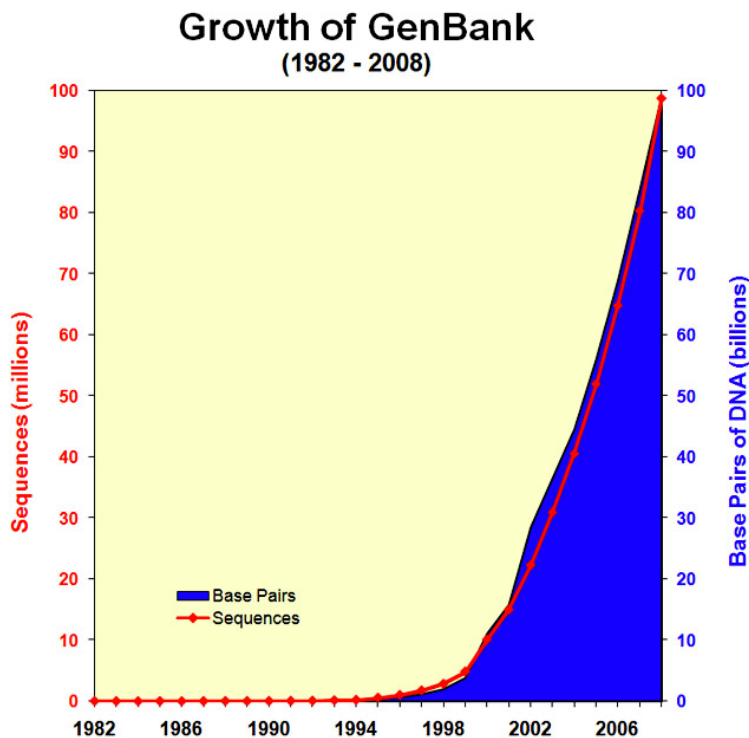


Figure 1. Growth of the publicly available gene-sequence database from its inception through 2008.³⁰ As of mid-2009 the number of sequences had reached 106,073,709 containing 105,277,306,080 bases.³¹ Note that for the purpose of this illustration, a “base pair” is synonymous with a base.

Concomitant with the move to encyclopedic coverage of all the functional components and processes of organisms has been the rapid growth of “Systems Biology,” a broad research category that stresses the applications of systems analysis to comprehensive datasets from biological systems. The growth of systems biology and several other contemporaneous revolutions in our understanding of the biological world has forced ambitious biologists to undertake computation-driven interdisciplinary approaches to their subject. Every Synthetic Biologist we interviewed described how the complex interactions of different parts of living systems demand a high level of sophistication in both understanding individual components and modeling their interactions and argued that much of the inspiration for Synthetic Biology came from the desire to engage in bioengineering that did not require

such a level of understanding for its success.³² Unlike modularly-designed synthetic systems, removing any component of a living organism can have varied and unpredictable effects: sometimes it kills the organism, sometimes it prevents reproduction, and sometimes it merely lowers the organism's fitness.

Modern SB fits under the systems-biology umbrella. It is a natural outgrowth of the expanded range of knowledge and possible experimentation resulting from DNA sequencing and from the detailed study and analysis of some of the billion or so sequenced genes. In this context, the motivating goals of synthetic biologists are twofold: (1) to confirm our understanding of how genes function by putting them to use in designed systems (many of which mimic the components of natural cells); and, (2) to use sets of genes to create novel engineered organisms with useful functions. The SB field thus straddles the divide between basic science and engineering with a preponderant emphasis on the latter.

Principles of Synthetic Biology

As with most modern technologies, including computer hardware design, SB is built around the concept of assembling useful devices from standardized components. The back-to-back publication of two papers in the January 20, 2000 issue of *Nature* can, somewhat arbitrarily, be said to mark the beginning of modern SB.^{33,34} The first paper, by a team from Caltech, reported successful construction of a genetic circuit, termed a “repressilator.” By linking three sets of regulatory genes together and using them to control expression of a fluorescent protein, the authors produced a strain of bacterial cells that could oscillate between states of high and low fluorescence output. This system mimics the properties of an oscillator, a key component of electronic circuits.

The second paper, by a team from Boston University, reported on the creation of a mechanism they dubbed the “genetic toggle switch” by inserting several genes into a small piece of DNA (called a “plasmid”) that can grow in *E. coli* cells. Plasmids are small, circular DNA molecules a few thousand bases long that can replicate in bacteria and represent a kind of auxiliary chromosome. They also usually have an antibiotic-resistance gene that protects the cells that contain them when the cognate antibiotic is

added to the culture. Thus researchers can insure that only the desired plasmid-containing cells will grow in their experiment. The researchers inserted two repressor genes that oppose one another's expression into the same cells. Each repressor makes a protein that binds to a short control sequence of DNA called a "promoter" that will be read before the gene for the other repressor is read. When the repressor protein binds to the control sequence, it blocks expression of the gene for the other repressor. The final components of this system that allow it to function as a toggle switch are two inducers – small, drug-like molecules that bind reversibly to specific repressor proteins and convert them to an inactive state. By adding one or the other of the inducers to a bacterial culture the matching repressor gets turned off and the genes it controls, including the other repressor, turn on. Adding the alternative inducer reverses the effect. The genetic toggle switch illustrates how the proper combination of only a small number of genetic regulatory elements can provide a fundamental component for the synthetic biologist's toolbox. This basic component can then be used in the construction of more complex and immediately useful biological systems.

The emphasis on modularity at the core of Synthetic Biology is the tale of the toggle switch writ large. Thomas Knight, Drew Endy, Jay Keasling and colleagues advance the principle of assembling useful complex devices from simple standardized genetic components as the core principle of SB. Knight defined this idea in general form: "The key notion in the design of our strategy is that the transformations performed on component parts during the assembly reactions are idempotent in a structural sense. That is, each reaction leaves the key structural elements of the component the same. The output of any such transformation, therefore, is a component which can be used as the input to any subsequent manipulation."³⁵ This means that properly designed SB devices will minimize the complex interaction problem that bedevils conventional genetic engineering efforts. This is an idealized goal, but one where even a partial success could yield substantial benefits.

The goal of Synthetic Biologists is to replace *ad hoc* experimental design with a set of standard and reliable engineering procedures to remove much of the tedium and uncertainty during assembly of

genetic components into larger systems. To encourage work on production of standardized biological parts with standardized means of assembly, some Synthetic Biologists have spearheaded the construction of what they call “BioBricks,” functional pieces of DNA designed to be easily assembled and interact predictably when made part of a larger structure. These BioBricks are registered within a publicly-accessible database called “The Registry of Standard Biological Parts” (<http://www.partsregistry.org>). Analogous to the interchangeable parts that were a cornerstone of the Industrial Revolution, BioBricks are meant to make the *de novo* construction of novel biological systems considerably easier, decreasing the time, expense, and skill level necessary to develop biological systems that can perform tasks as varied as producing artemisinin (a costly, difficult-to-conventionally-synthesize component of an effective anti-malarial drug therapy), making cellulosic biofuels, or seeking and destroying tumors. The ability to modify biological systems in this way could have a massive and wide-ranging impact, transforming significant sections of the world economy.^{36,37} In theory, modular standardized biological parts based on principles similar to those underlying BioBricks could be employed to create biological weapons, but it might also help improve defensive capabilities against both natural and artificial biological threats.

Potential effects on offense³⁸

A biological weapon is a system with four components: the biological agent itself, additives that protect the agent while it is stored and after it is dispersed, a munition that transports the weaponized agent, and a mechanism to disperse the formulation onto or over the targeted population. Producing a biological weapon takes five steps: acquiring a suitable agent, scaling up production or magnifying the agent to generate usable quantities of it, weaponizing the agent and methods of dissemination of the agent, manipulating physical characteristics and developing munitions, and controlling effects of the agent on targets and on one’s own forces.

The general advance of biotechnology, and especially the increased speed and lower costs of DNA synthesis, is likely to have implications for each of these processes. We focus, however, on the marginal impact of DNA synthesis and SB, not the overall impact of technological progress. DNA synthesis is likely to have its largest and most immediate impact on Acquisition. In the medium and long term SB may have substantial indirect effects on the Magnification and Weaponization stages by allowing the use of different agents or agents with different properties. In the long term (i.e., more than 10 years) SB may have its largest impact on the Effect stage by facilitating the creation of agents with novel characteristics.

1. Acquisition

The first step in constructing a biological weapon is the acquisition of a suitable agent. Many such agents would be difficult or impossible even for states to acquire, and even more difficult – perhaps impossible – for non-state actors to do so. Stocks of *variola* virus, the causative agent of smallpox, for example, officially exist only in the United States’ Centers for Disease Control (CDC) in Atlanta and in Russia’s Vektor, both secure research facilities.³⁹ Acquiring a sample of the *Ebola* virus would require considerable skill at field biology.⁴⁰ Even agents that seem easy to obtain can pose surprising difficulties. *Bacillus anthracis*, the bacterium that causes anthrax, is widely available in the natural world, but most natural strains are not particularly dangerous.⁴¹ When the Aum Shinrikyo cult attempted to launch an anthrax attack in Tokyo it used a strain that was not dangerous to humans, which was only one among many failures in its biological weapons program.^{42,43} Perhaps most strikingly, the virus that caused the 1918 influenza pandemic was not added to the CDC’s list of select agents until 2005 because it was unavailable to anyone under any circumstances because it no longer existed in any form, either in the natural world or in storage.⁴⁴ Even its genome sequence was unknown. Extraordinary work in forensic biology, however, has allowed the virus’s genome to be determined and reconstructed from the remains of some of its victims buried in Alaskan permafrost.⁴⁵

DNA synthesis technology is improving at exponential rates – faster, in fact, than the well-known Moore’s Law which governs computer performance.⁴⁶ Such improvements may allow the acquisition of biological agents through synthesis, potentially broadening the pool of actors able to acquire such agents.⁴⁷ This technological shift may change the relative, as well as absolute, danger from different potential agents. In general, viruses will be considerably easier to synthesize than bacteria due to their smaller genomes and simpler structure.⁴⁸ While virus genomes usually need relatively little support structure to become active agents, a bacterial genome needs all of the other apparatus of a bacterial cell, and virtually all the bioengineers we interviewed, particularly during follow-up interviews that focused specifically on this question, felt that inserting a bacterial genome into a cell in such a way that it becomes viable requires a high degree of laboratory skill and is likely to for the foreseeable future.⁴⁹ It is not, however, universally true that synthesizing viruses will be considerably easier than synthesizing bacteria. *Variola*, although a virus, has both a very large genome and requires a highly complex and difficult-to-synthesize protein coat, both of which make it a very challenging target for *de novo* synthesis despite its other attractive qualities as an enormously lethal biological weapon. Several experienced bioengineers suggested that using a helper virus to generate the protein coat might circumvent some of these difficulties, although probably at the cost of great risk to the experimenters.⁵⁰

Given the rate at which DNA synthesis is progressing, relatively easy *de novo* synthesis of some viruses is likely to be a feature of the short and medium terms (less than 10 years in the future). This is particularly likely given that the first artificially constructed virus, the polio virus, was synthesized in 2002.⁵¹ This may expand the pool of organizations able to acquire agents suitable for biological weapons. Groups that lack field biology skills or the ability to differentiate between different strains of the anthrax bacillus might nonetheless be able to synthesize viruses, potentially even through commercial DNA synthesis companies – though cooperative efforts initiated by the companies themselves now provide software that can identify potentially dangerous sequences.⁵²

Moving beyond DNA synthesis, however, SB techniques may further complicate the issues surrounding agent acquisition in the medium (5-10 years) and even more likely, long (10+ years) terms. They may do so in two ways: by allowing the easier modification of natural agents, and by enabling the creation of entirely new organisms, particularly those with novel properties. Natural agents that currently have little or no pathogenicity might be much more easily modified into suitability as biological weapons using SB. Dual-use SB parts and devices might conceivably be more easily inserted into natural viruses than conventionally engineered genes, perhaps allowing them to evade biosensors, vaccines, or other therapies. These chimeric organisms (hence the title of this paper) could combine the qualities of several different organisms, each of which has some traits which an attacker would find attractive, even if no accessible natural organism exhibits all of these characteristics. This ability to alter natural agents could modify the already large roster of agents suitable for use as biological weapons to include almost any virus or, in the farther future, bacterium.⁵³

Creation of entirely synthetic agents – ones without natural analogues – although still further in the future, could expand the universe of potential threats still more by, for example, allowing potential attackers to modify synthetic viruses used for medical purposes into weapons. Three of the synthetic biologists we interviewed in our initial screening, and several others during follow-up interviews, suggested that some of the already published work in SB sets up systems that malicious actors might attempt to modify by straightforward procedures to produce potential bioweapons.⁵⁴ These already rank among the more sophisticated projects in cellular engineering, so this approach would currently require considerable talent and resources, but further progress in the field may make it considerably easier in the future. PCR (Polymerase Chain Reaction), after all, a technique for DNA sequencing whose discovery merited a Nobel Prize, can now be performed by an advanced high school student.

2. Magnification/Amplification

Magnification or amplification of potential agents to produce a volume of pathogens suitable for use in an attack also requires significant resources and nontrivial skill. The production of large amounts of bacteria requires specialized and expensive equipment, while the growth of large quantities of viruses requires bioreactors or “thousands of virus-free [chicken] eggs.”⁵⁵ Advances made in other areas of biotechnology may substantially ease the difficulty of magnification because the production of viruses in quantity is useful for some medical applications.⁵⁶ Advances in DNA synthesis and SB, however, are likely to have only second-order effects on this hurdle. Non-contagious agents like the anthrax bacillus require large amounts of magnification because every victim must be infected in the original attack. Contagious agents, on the other hand, can self-magnify after an initial attack. This means that non-state actors interested in large-scale attacks are much more likely to rely on such agents, despite the greater difficulty and risk involved in handling them before the attack. DNA synthesis and SB are most likely to affect Magnification by making it easier for potential attackers to acquire highly contagious agents.

3-4. Weaponization and Dissemination

These two phases are taken together, as the effects of SB on them appear to be identical. Weaponization of biological agents usually involves formulating them for maximum stability and ease of delivery in aerosol form, as aerosols are the most effective way to infect large numbers of people. An aerosol requires both a munition and an agent. The munition is the system which converts the agent into an aerosol form and then disperses it at the target area. Both must meet a fairly demanding set of technical requirements. The agent must form droplets of the correct size to allow it to remain suspended in air and to reach deep enough into the lungs to become infectious, while also being sturdy enough to survive storage and transport. The munition must be able to disperse the agent effectively, must not destroy the agent in the process, and must produce particles of the correct size.⁵⁷

As with other stages of the weapons-manufacturing process, technical progress outside of DNA synthesis and SB is likely to continue to make weaponization easier as the skills and techniques involved spread beyond the weapons community.⁵⁸ The recently withdrawn drug Exubera, for example, required converting an insulin powder into an aerosolized spray which could be inhaled, delivering insulin into the bloodstream of a diabetic through the lungs. The relevance of such technologies to someone attempting to create a biological weapon is obvious.

Here too SB is likely to have only second-order effects and those will be further in the future than its effects on other stages. SB could potentially help potential attackers by allowing them to modify the traits of their selected agents to make them more suitable for weaponization. A specific example might be the creation of novel engineered bacterial pathogens that form spores in the same way that anthrax does, thereby producing a stable, concentrated powder to use in attacks. All interviewed Synthetic Biologists, however, agreed that such fine control over the properties of agents is more likely to occur in the long term.⁵⁹

5. Effect

SB is likely to have its largest impact in this phase, although it is unlikely to appear in the short or medium term. Natural pathogens suitable for biological attacks provide the ability to kill people (like *Variola* or *B. anthracis*), sicken them for short periods of time (like the *Salmonella* bacteria used in the Rajneeshee cult's attack in Oregon), or cause economic harm through attacks on agriculture and livestock (foot and mouth disease, sometimes known as hoof and mouth disease, for example, is ideal for this). Every interviewee agreed that the most-important long-term offensive implications of SB will be found in its ability to provide potential attackers with a much broader variety of potential new effects. These can be broken down into three categories: enhanced lethality, enhanced infectiousness, and "wild card" applications.

Many highly contagious agents, such as the various viruses that produce the common cold, are unsuitable for use as biological weapons because of their limited effects on those they infect. Conventional genetic engineering techniques have already been used to enhance the lethality of some agents. The most famous case, however, that of mousepox with the gene for the expression of interleukin-4 (IL-4) added, actually illuminates the difficulties with these approaches. In 2000 researchers in Australia inserted the gene for IL-4 expression into mousepox not to increase its lethality or cause it to evade the mousepox vaccine but in an attempt to stimulate the production of antibodies against mouse eggs to render the mice infertile. Instead of the intended effect, the researchers discovered that this engineered mousepox completely suppressed the animals' immune response to viral infections. Normal mousepox usually causes only mild symptoms in the type of mice used in the study. The engineered mousepox, however, killed every single unvaccinated mouse in nine days, even killing half the mice who had been vaccinated against mousepox. The researchers believe that performing the experiment on smallpox would have the same results in humans.⁶⁰

Perhaps the most significant aspect of this experiment is the unexpectedness of the result. Before these results were reported, most researchers had believed that modification of viruses would tend to make them less, not more, dangerous.⁶¹ This unpredictability, however, would be a significant handicap for an organization with limited resources attempting to create genetically modified harmful biological agents. Most attempts to modify naturally occurring pathogenic agents have no dangerous implications and so never come to the attention of those outside the research community. Thus most observers are likely to overestimate the likelihood of such experiments having biowarfare implications.⁶² A sub-state actor, or even a state with limited resources, may have considerable difficulty using conventional genetic engineering techniques to change or enhance the effects of natural biological agents.

SB promises to affect this calculation in two ways. First, techniques ranging from large-scale DNA synthesis to automated assembly are likely to substantially decrease the cost of attempting to modify natural organisms, allowing potential attackers to make many more attempts with the same level

of resources. Second, one of the central thrusts of the SB project is precisely to reduce the element of uncertainty in modifying biological systems to produce desired characteristics by creating standardized and well-characterized parts available to any researcher. SB may thus allow attackers attempting to modify agents to increase their lethality or infectiousness more predictably, instead of depending on a fluke experimental result like that which produced IL-4 mousepox.

Perhaps most important, though, are potential “Wild Card” changes to the effects of biological agents. SB’s emphasis on modularity creates the potential for sudden rapid changes in the threat environment because of the possibility of combining seemingly unrelated technical developments in unpredictable and significant ways.

For example, the Synthetic Biology Engineering Research Center (SynBERC), a major National Science Foundation-sponsored project devoted to the development of foundational technologies in SB, is seeking to develop tumor-killing bacteria as a potential early application of SB.⁶³ Such artificial bacteria must be invisible to the human immune system if they are to work effectively. If they are designed according to the principles of SB, they must also be relatively easy to modify. In and of themselves, such bacteria would have little application for potential developers of biological weapons. A second major early application of SB is the synthesis of high-value chemicals like those in pharmaceuticals, a potential already demonstrated by the synthesis of artemisinin. Zolpidem, the active ingredient in Ambien, can reliably and relatively safely put most people to sleep. The use of SB to develop a molecular pathway which synthesizes Zolpidem or a molecule with similar biological effects is easily imaginable. Again, by itself, this discovery would have little impact on biosecurity.

Interactions between these two hypothetical discoveries, however, could have significant security implications. Imagine taking the immune-invisible tumor-killing bacterial chassis, deleting those sections relevant to cancer treatment, and inserting SB components that produce sleep-inducing chemicals and make the bacteria capable of infecting subjects through the air. Combining such disparate discoveries would have been a major research effort with uncertain results using traditional genetic engineering

techniques because of the unpredictable interactions between the host bacterium and the new metabolic pathways. This new bacterium could potentially be a reliable and safe airborne sleep-inducing agent, something which no government currently possesses but which has obvious utility. By its very nature the SB enterprise, if it succeeds, will make such combinations considerably easier. This example is only one of many possible such effects. Biological agents could be designed to alter behavior, cause long-term chronic conditions, or perhaps even target specific ethnic groups by interacting with particular foods or genetic markers. There is evidence, for example, that some infectious diseases subtly influence the behavior of humans who carry them.⁶⁴ Agents might even be made more controllable by combining them with counters designed to restrict the number of cell divisions, effectively “cleaning up” the locus of an attack, or designing them with highly specific cures known only to their creator.

The ability to create agents with such unique effects is almost certainly a long-term (10+ years) proposition. All interviewed experts agreed, however, that if SB succeeds, it is highly likely, perhaps even almost certain, to make it possible to construct such customized biological weapons.

This possibility has two significant secondary security implications. First, it is likely to significantly increase the incentives for states to conduct research on offensive biological weapons – an activity easily disguised with claims that the research is purely defensive. One of the major reasons for the United States and Great Britain’s unilateral abandonment of offensive biological weapons research was their feeling that such weapons had little or no utility for states already armed with nuclear weapons, because biological weapons were far less reliable and controllable than their nuclear counterparts.⁶⁵ Advanced customized biological weapons, however, have the potential to be both more controllable than their unaltered counterparts and to give users capabilities that they could not otherwise possess. Governments, perhaps facing considerable pressure to use non-lethal agents in situations ranging from crowd control to suppressing terrorism, may decide that new biological weapons are the only way to deal with these demands. Once the taboo against biological weapons of any sort has been broken, even by non-lethal agents, it is easy to imagine the slide into further research on far more malevolent applications.

Researching and using such agents may also deepen the pool of people with access to the skills and equipment needed to move through every stage in the development of a biological weapon. Finally, the difficulty of distinguishing between offensive and defensive biological weapons research means that a spiral dynamic, already a concern given the United States' aggressive biodefense research program, seems likely to be further heightened.^{66,67}

Potential Effects on Defense

Although the term “dual-use” normally precedes a discussion of a technology's abusive applications, it also implies positive ones. In the case of SB some of these uses can directly counteract potential abuses. These include: Sophisticated, novel methods of surveillance for bioweapons; Faster, more-targeted production of vaccines and other means of enhancing immune-system function; Improved development and production of antibiotics, both natural and synthetic; and, “Blue sky” techniques to fight pathogenic organisms with defensive organisms that have no harmful effects on humans, animals, plants, or benign microbes.

This list is not intended to be comprehensive, though it probably includes most of the foreseeable possibilities. In what follows we briefly review each of these categories. The impact of SB in these cases will depend on the degree to which it develops as a mature technology. SB's impact on the development of new vaccines and therapeutics is particularly uncertain. The development of new drugs and vaccines is subject to an extraordinarily high failure rate; this is one of the primary drivers behind the extraordinarily high cost to develop new drugs.⁶⁸ Despite this, all six of the synthetic biologists who were among our primary interviewees expressed great optimism about SB's potential to eventually make significant contributions to such defensive approaches, and several noted that it has already begun to help with the production of validated molecules. In follow-up interviews subjects sometimes expressed some doubts as

to how soon SB could help with the creation of new therapies and vaccines, but echoed the initial interviewees' confidence that the technology was likely to eventually produce such benefits.⁶⁹

Improved surveillance

Surveillance to detect pathogenic agents in a population takes two basic forms: (a) classical epidemiological analysis of the distribution and symptoms of the victims of infectious disease (supplemented by syndromic surveillance techniques,) and (b) physical detection of the agents themselves. The latter process requires sensitive, specific chemical or biological probes capable of discriminating true pathogens among a background of related microorganisms. Such probes usually derive from immune system components, mostly antibodies. These can be coupled to techniques that translate molecular recognition by the antibody into spectroscopic signals, typically fluorescence.

Conventional means for developing specific and sensitive antibody-based sensors involve lengthy, *in vivo* procedures that prevent a rapid and flexible response to novel pathogens. SB techniques, however, may allow much faster responses by engineering libraries of modified antibodies that can be screened via high-throughput methods to select optimum binding, stability, and other characteristics. They also can couple the sensor molecules to versatile and inexpensive cell-based signal-output devices. Some prototype systems designed for other types of targets have been developed by undergraduate student teams for an international competition. For example, one student group has proposed an arsenic sensor that can be built remarkably inexpensively and operates under field conditions. Such developments bode well for designing systems to detect pathogens.⁷⁰

Accelerated vaccine production

The lag time for development of a vaccine for a novel pathogen has typically been measured in years. In cases where the causative agent is familiar and changes gradually by mutation this may be reduced to months. For DNA vaccines to combat seasonal or pandemic influenza, one company now

claims to be able to produce effective vaccines in a matter of weeks.⁷¹ DNA vaccine technology could be enhanced by SB through design of more effective and versatile cell lines to express a wide variety of vaccines in suspension culture.

Most discussions of bioweapons focus on agents that are contagious and highly lethal. Chronic infections (like HIV or hepatitis C) seem unlikely candidates for use as weapons, though they might have a greater impact since they would presumably wreak havoc for decades. The root cause of the chronic nature of such diseases is that the agents' epitopes (chemical surface features that provoke antibody formation) fail to elicit a strong immune response. Design of vaccines to combat such agents requires engineering features that enable the vaccine to generate a more potent immune response.⁷² SB techniques provide an ideal toolbox to accomplish this goal. Engineered adjuvants – that is, chemicals added to a vaccine to magnify the immune response it provokes - might also be generated more effectively using SB techniques.⁷³

Development and production of new antibiotics

Antibiotic resistance is a key feature of some pathogens that potential users of biological weapons may seek to exploit. Anthrax, for example, which in its natural state is usually vulnerable to a wide variety of antibiotics, might be modified to include a multiple antibiotic resistance gene cassette. Drug development for antibiotics tends to be slow and costly because it relies on chemical leads expanded into libraries of compounds to be screened. The organic synthesis of antibiotics (especially those based on novel leads) can be a slow process, and once a set of key related compounds has been chosen for further study scale-up often takes an additional year or more since the research-scale syntheses are seldom suitable for large-scale production. Pharmaceutical companies developing antibiotics must also deal with the waste created by the generation of side products in a chemical synthesis.⁷⁴

Metabolic pathways have a number of key advantages over traditional chemical synthesis in the production of complex organic molecules. Conventional methods of producing these molecules can be

inefficient because they produce stereo-isomers of the desired compound. Stereo-isomers are molecules with the correct formula but a mirror-image geometry that renders them biologically inert. Conventional chemical production is usually a multi-stage process during which 50% of material can be lost at each stage, because half is converted to waste isomers. Enzymes, however, are stereo-specific. They act only on molecules with a specific geometry. SB may enable much easier use of engineered enzymes in the production of complex organic molecules, eliminating the waste due to stereo-isomer production and vastly increasing yields. Similarly, production via a fermentation-type process using an engineered producer strain offers significant cost advantages. Given sufficient advances in SB techniques, if a new type of organism were to be identified for which no available antibiotic is effective, metabolic engineering via SB techniques might shorten the period necessary to develop a new therapy for it. Developing a repertoire of novel antibiotics, some of which could be held in reserve, would be one of the best ways to prepare for potential bioterrorist attacks. The leverage to increase the size and scope of antibiotic-development programs that SB will eventually afford is likely to be a significant advantage to defenders against biological attacks and, of course, natural diseases as well.

Defensive approaches based on engineered organisms

Synthetic Biologists may also seek to develop entirely novel therapies for some pathogens. Elaboration of variant forms of natural immunity could play an important part in combating infectious diseases. For example, a normal bivalent antibody (IgG) with two identical binding sites might be converted into an antibody with two heterotropic (non-identical) sites that bind to different ligands (sites on biological molecules to which other molecules, like antibodies, can attach themselves). Such antibodies, produced by engineered organisms, could couple binding to a pathogen with interactions with some cellular immune system components such as macrophages. This could enhance immune response. Approaches of this type may have potential as a cancer therapy as well as in biodefense.⁷⁵

Conceivably, bacteriophages (viruses that infect bacteria) could be created to specifically attack engineered pathogens, though this therapeutic approach, first proposed many years ago, has not yet reached the stage of clinical practice in the United States.⁷⁶ A report on the protective effect of a strain of *Lactobacillus casei* against chemically induced ulcerative colitis in mice provides a prototype example for possible roles of engineered bacteria as potential therapeutic agents.⁷⁷

The SynBERC testbed aimed at engineering bacterial cells to target tumors where they can inject toxins to kill the cancer cells represents a similar approach. A 2006 student project from Slovenia demonstrated the potential feasibility of an engineered therapy for sepsis, a common component of bacterial infections. Projects like these represent preliminary results at the moment, but they nevertheless justify optimism that SB will lead to an era where powerful defensive tools can be developed much more rapidly than now.⁷⁸

Implications of Deskillling and Diffusion

Every initial interviewee who worked specifically on synthetic biology suggested that one of its most important aspects is its combination of the de-skilling of biological engineering and creation of techniques to alter living systems using modular design. This was unanimously affirmed by Synthetic Biologists in follow-up interviews.⁷⁹ These two efforts are linked in many ways. Altering non-engineered living systems using conventional recombinant DNA techniques currently requires significant degrees of tacit knowledge. Tacit knowledge is knowledge primarily gained from experience instead of formal education. Tacit knowledge in biology is usually acquired through prolonged apprenticeships with senior scientists. This is essentially a cottage industry within academic and commercial biotechnology. Such tacit knowledge is currently among the most significant barriers to bioweapons proliferation. Even the creation of a synthetic poliovirus from commercially available segments of DNA required significant tacit knowledge.^{80,81}

The advance of technology normally converts tacit to explicit knowledge over time. During the First World War, for example, France's key artillery piece was a 75mm gun. Desperate to replace the production from factories lost to German armies, the French sent the highly secret blueprints to American factories to allow them to manufacture the weapons. These factories, however, were unable to produce guns of sufficient quality until a team of French workmen were sent to show the American factories how the guns were made.⁸² The American factories simply lacked the tacit knowledge not conveyed in the blueprints. Today, however, all that a sophisticated factory would need is an emailed CAD file. The normal progress of biotechnology may "replace or...alter the kind of tacit knowledge required for bioweapons development..."⁸³ It also may not, and so far it has largely failed to do so.

Synthetic biology is unique, however, in the extent to which it is *explicitly devoted* to the minimization of the importance of tacit knowledge. For example, interview subject A, a founder of synthetic biology, said that "It is probably right that synthetic biology is decreasing the tacit knowledge needed to do biological work. It's a major goal for me to remove that lore."⁸⁴

SynBERC in particular has focused upon the elimination of tacit knowledge from the manipulation of living systems. It structures its research around a hierarchy of standardized biological parts, devices, and chassis, which are meant to allow for the easily-replicable creation of biological systems with artificial properties. In an overview of SynBERC, center Director Jay Keasling described the high demands for tacit knowledge that currently hinder even the most skilled bioengineers and said that SynBERC's "Vision" is "to make biology easier to engineer."⁸⁵ The emphasis here is crucial. SynBERC certainly seeks to produce various specific applications, but that is not its primary goal. Instead it seeks to eliminate the barriers, particularly those involving tacit knowledge, that make it more difficult for *everyone* to engage in successful bioengineering. For example, researchers affiliated with SynBERC are working on both automated cloning and automated assembly of DNA segments, while others are developing software for the computer-aided design of living systems.⁸⁶ Although these and other such attempts may fail, or succeed only in part, they mark a crucial and fundamental divide between

synthetic biology and traditional bioengineering. SB includes, as a principal part of its agenda, a sustained, well-funded assault on the importance of tacit knowledge to bioengineering and thus on one of the most important current barriers to the production of biological weapons.

This de-skilling is complementary with SB's emphasis on modularity. As mentioned earlier, one of the principal difficulties in modifying living organisms using conventional techniques is the interaction between different genes, resulting in unanticipated effects when an altered gene has unanticipated functions or affects the functions of other genes in unknown ways. The probability of such unintended consequences rises exponentially with the number of genes altered, so that few genetic engineering applications have involved changes in more than a handful of genes. By contrast, Amyris Biotechnologies' project to produce artemisinin commercially in yeast using SB techniques involved the alteration of 16 genes.⁸⁷

SB attempts to eliminate these interaction effects by creating standardized modular biological parts. These parts are meant to be insulated from interaction with other parts of the biological system. It is likely that organisms designed using such techniques will face significant performance costs when compared to natural, fully-integrated systems. A similar phenomenon occurs in businesses, where tightly integrated organizational structures are more efficient, but much harder to alter, than modular ones.^{88,89} Nonetheless, if these efforts bear fruit they will make the alteration of biological systems vastly faster and less expensive, an effect that is magnified by the combination of the two technologies.

De-skilling and modularity are thus likely to have two effects beyond the ones already specified. SB is likely to eventually greatly expand the universe of capabilities open to its most skilled practitioners. With sufficient resources, skilled genetic engineers using conventional techniques could already make significant contributions to an offensive bioweapons program. De-skilling and modularity, however, have the potential to both rapidly increase the diffusion of skills and decrease the skill gradient separating elite practitioners from ordinary ones. Diffusion will increase because the investment in time and resources necessary to acquire the capability to manipulate living systems will decrease as the training and

experience necessary to do so drops. Thus new actors are likely to gain this ability. Similarly, the high degree of tacit knowledge involved in traditional genetic engineering means that today less-skilled practitioners can have significant difficulty replicating the achievements of elite ones, even if all the necessary data has been published. These same two traits of SB are, however, likely to make replication of these achievements vastly easier, substantially leveling the gradient between elite and peripheral practitioners.

Another dimension to the de-skilling/diffusion aspect of SB comes from the effects of efforts by synthetic biologists to encourage internationalization of their field. Of the first four annual conferences devoted to SB, two were held outside the United States, one in Zurich and another in Hong Kong.⁹⁴ Another rapidly growing activity has been the “International Genetically Engineered Machines” competition, known as “iGEM.” iGEM involves undergraduates and graduate student teams in synthetic-biology projects. Thousands of students from more than 20 different countries (and nearly 100 colleges and universities) have been initiated into the procedures of SB, not only developing a baseline competence but also acquiring self-confidence and enthusiasm about their ability to engineer organisms. Table 2 shows the remarkable growth in iGEM’s global participation. To these practitioners we can also add the gradually increasing flow of PhD graduates and post-doctoral fellows who have trained in SB research laboratories and subsequently pursue careers in other locations, frequently in other countries. Thus the number and geographic distribution of practitioners of this new technology is likely to grow substantially over time.

Finally, the potential of so-called “garage biohackers” is gaining some attention, particularly from members of the synthetic biology community. Our interviews revealed a distinct split in the SB community on this point, with some SB researchers notably enthusiastic about the prospect of a “garage biotechnology industry,” while others doubted both the possibility and the desirability of such a thing coming into existence in the foreseeable future.⁹⁵ Much like the now-legendary pioneers of the personal computer revolution, amateur synthetic biologists are beginning to wax enthusiastic about conducting SB

experiments at home. DIY (do-it-yourself) biology has recently become quite popular, especially online.⁹⁶ Although there is currently no evidence of any malicious intent by anyone involved in this community, the potential for a hacker culture that replicates some of the less desirable traits of that surrounding computers cannot be dismissed out of hand.

At the present time the DIY biologists operate at a simple level and often display naiveté about many molecular biology laboratory basics.⁹⁷ Part of the fun appears to be improvisation and the sense that it might be possible to “clone on a shoe-string.” The possibility of serious harm coming from the biohacker culture currently seems remote, given both a lack of desire and capability on the part of today’s experimenters. However, a committed individual of only modest means could equip a home laboratory with all of the key pieces of equipment for performing SB experiments by buying from used equipment dealers, or simply eBay. Katherine Aull, for example, a recent graduate of MIT, entered the perhaps too-appropriately-named “Mad Science Contest” sponsored by io9, a popular website. In her submission she described her work developing a biological counter using only the equipment she had assembled inside the closet of her apartment in Cambridge, Massachusetts.⁹⁸ Notably, her design uses the genetic toggle switch described earlier in this paper as one of its key components – a perfect example of the cumulative nature of the synthetic biology project. Over time such homegrown capabilities will doubtless grow. Naturally, the more advanced training and molecular biology skill the hacker has from high school or college courses, the more ambitions his or her agenda might become. At present it remains a stretch to imagine that some of the more lurid fictional possibilities might be realized.^{99,100} But 10 years from now, this could change.

Policy Recommendations

Improving biosecurity has been a focus of governmental agencies and the policy community since the attacks of September 11 and the anthrax attacks the following month. Because of their unique

characteristics, including their lethality and invisibility, biological weapons are particularly likely to cause fear in target populations and produce sharp reactions and overreactions to potential threats.¹⁰¹ Despite the lack of significant numbers of casualties from biological weapons use, the United States government has devoted considerable resources to researching how to protect its citizens from them, spending more than \$40 billion on biodefense since 2001.^{102,103,104,105} Biological weapons in the hands of non-state actors are a matter of particular concern, both because they may combine relatively low start-up costs with the ability to cause mass casualties and because defending against such attacks takes significantly more resources than launching them.¹⁰⁶ Finally, biological weapons present policymakers with an almost unique degree of uncertainty, as expert assessments of them can vary on almost every significant factor, ranging from the motivation of attackers to use biological weapons, to the feasibility of doing so with current technology, to the specifics of what agents and targets might be selected by potential attackers.^{107,108,109}

So, what is to be done?

As our focus is specifically on synthetic biology and its biosecurity implications, not the larger question of all security issues related to biotechnology, it focuses on measures specifically related to this new field of science and engineering. All interviewed experts agree that biological weapons pose the only potential rival to nuclear weapons in terms of destructive capacity and that, as reported by the Graham-Talent Commission on WMD proliferation, an attack using biological weapons is substantially more likely than one using nuclear weapons.^{110,111} The most important medium-term offensive impact of SB is likely to be its potential to lower the level of skills necessary to acquire or synthesize an agent. The combination of de-skilling and modularity may significantly increase the universe of people with the capability to alter agents in ways useful to potential attackers.

Fortunately, there are several promising policy options available to minimize SB's offensive potential and maximize its contribution to biodefense. Life scientists in general are "alarming[ly]" disengaged with the potential security implications of their discoveries.¹¹² The SB community, however,

is a notable and laudable exception to this trend. The major annual SB conferences have consistently featured speakers presenting on security issues; SynBERC includes a “Human Practices” research component that has security implications as one of its primary foci; and in Europe the SYNBIOSAFE program is involved in a similar endeavor.

This active discussion of the security implications of SB, combined with the heightened interest in biosecurity since the anthrax attacks of October 2001, has led to a wide array of sometimes highly-innovative approaches to maximizing SB’s contribution to biosecurity. These approaches can be divided into four categories: Community, Regulation/Surveillance, Research, and Design. All of these revolve around the idea of increasing the obstacles and resources necessary to craft a bioweapon using SB techniques. None by itself is a cure-all, in fact, all of them combined are unlikely to make offensive uses of the technology impossible for highly skilled or well-funded groups. By making the task more difficult, however, they can eliminate the threat from less capable actors and push back the time at which even more capable actors will have access to the full panoply of modalities offered by the new science, buying time for its potential beneficial applications in the hands of defensive-minded governments to overcome its threatening offensive potential.

All interview subjects emphasized that, although the odds of an improper use of synthetic biology techniques are infinitesimal in the near future, and very small for considerably longer than that, any such incident would have a devastating impact on the future of the research community, and even that of the technology itself. This could well be true even if the actual harm was negligible, as is most likely from any such incident.¹¹³ The potential for harm to the field is a powerful argument, however, with which to convince current and aspiring synthetic biologists of the importance of considering the security implications in their work, and should be part of the standard SB curriculum.

Community

Interview subject B suggested that the creation of a SB professional organization that devotes significant resources to raising awareness of and creating community norms about biosecurity issues is a crucial component of defusing the new technology's offensive potential. As did other interview subjects, he described several potential advantages that such an institution could bring. These include: Inculcating norms against working on bioweapons; Providing alternative means of support for scientists who are assigned tasks which they find ethically questionable; Fostering stronger community bonds that could help provide alerts about possible offensive programs; and, Enabling and giving more force to community codes of conduct.

Several synthetic biologists, as well as several experts who focus primarily on traditional biosecurity, recommended a series of steps to create a safe and open culture within synthetic biology. For example, subject F recommended that, starting with the lowest educational levels and extending to the top of professional societies, the field should put great effort into generating norms of community, mutual support, and open communication. Insofar as is possible, he recommended developing "bottom-up" efforts to educate and socialize laboratory scientists in SB. This might be done in the spirit of the DIY biology community. Imposition of rules from the top, in the same way that radiation safety training is conducted, might be necessary for some basic details, but the sense of ownership of the issue should reside with the laboratory workers themselves. Part of that culture should include debunking the many ill-informed proposals that crop up on the Internet. There appears to be a certain cachet to blogs that discuss how easy it might be to build a bioweapon, as illustrated, for example, by Paul Boutin's piece "Biowar for Dummies."¹⁴

Interview subject B recommended banning secret research on bioweapons, even for "defensive" purposes. He suggested that government biotechnology programs should be completely transparent, a noted contrast from the Bush Administration's approach of vastly intensifying its classified research on

biodefense.¹¹⁵ Although we agree that the United States government's current posture vastly over-emphasizes the need for secrecy, we feel that the close kinship between offensive and defensive biological warfare research necessitates maintaining at least some secrecy around government defensive programs. The United States can and should, however, take steps to mitigate both the dangers of scientists within its own program going rogue – as occurred with the October 2001 anthrax attacks – and the potential that other nations will confuse its defensive program for an offensive one. Security background checks and psychological screening of those involved with the defensive program should be conducted much more thoroughly than they were before the anthrax attacks. All biodefense research should be conducted as openly as possible, with an emphasis on ensuring that scientists from close allies are included, and all such facilities should be located on campuses open to non-citizens, even if specific buildings are restricted.

Scientists currently are surprisingly ignorant of the terms of the Bioweapons Convention - a problem community organization could help solve.^{116,117} There are important reasons not to overrate the capabilities of such an organization, however. The closed communities typical of those research programs which have historically sought to develop bioweapons have demonstrated extraordinary resistance to outside norms.¹¹⁸ Relying on such organizations as a primary or principal means of defense against the offensive use of these technologies could thus increase the potential danger by creating a false sense of security among watchdog groups. As long as it is understood that community norms and community organizations are a secondary barrier - one intended to reinforce, not replace, first-line defenses – they could provide non-trivial benefits at negligible cost.

We also recommend the adoption of the “safety hold” norm as used by Air Traffic Control (ATC) systems. Proposed changes to ATC systems can be blocked by any member of the community who believes that they are likely to cause safety concerns.¹¹⁹ Creating such a norm in the SB community, one in which any member, even the least-senior undergraduate, can hold up an experiment by invoking safety or security concerns, could introduce a valuable new check within the community. Similarly, campus

Safety Officers and Institutional Review Boards should begin to consider SB experiments one of their responsibilities. Interview subject G stressed the need for laboratory researchers to have a known, confidential, well-informed Institutional Review Board to advise them on biosecurity-related issues.

Regulation/Surveillance

One of the key choke points for the offensive use of SB by sub-state actors may be the existence of large-scale centralized DNA synthesis. Most large DNA synthesis is currently done by a relatively small number of companies. The government could conceivably subsidize large-scale synthesis or impose reporting requirements on DNA synthesizers sufficiently burdensome as to discourage the development of “desktop DNA synthesizers” capable of making DNA fragments useful to attackers. Many of the leading DNA synthesis companies and the most prominent researchers in the field of SB have joined together to create the International Consortium for Polynucleotide Synthesis (ICPS), which is meant to enhance the safety and security of DNA synthesis. They have suggested the “development and validation of a tiered screening process that clearly identifies the contributions to safety and security due to user responsibilities, corporate practice and corporate technologies.”¹²⁰ This would include the requirement that those ordering synthesized DNA must identify themselves and that companies must use approved screening software to ensure compliance with all regulations.¹²¹ Similarly, the Sloan Foundation funded a wide-reaching study to assess the security implications of DNA synthesis and laid out a commitment to screening orders among one of a list of 20 options to improve safety and security.¹²²

Such measures are helpful but are, as yet, strictly voluntary. The fact that at least one major DNA synthesis company does not screen incoming orders is an open secret in the SB community.¹²³ This suggests that before DNA synthesis reaches a point where full viral genomes can be commercially ordered, regulations should be in place that impose safety and security standards similar to those proposed by the ICPS. Since the legal framework for such regulation is national, the only way to prevent a “leaky”

system would be to implement international agreements where all parties accept the same standards and sanctions.

Additional measures might also be implemented to address potential weaknesses in screening software. Parts of SB are characterized by a “hacking” culture. Instead of attempting to suppress this facet of its culture, there are some ways in which it might be adopted to help with security problems. For example, DNA synthesis companies could cooperate to create a pool of funds with which to reward hackers who successfully get hazardous sequences past the screening software and publish their results, allowing the software to be improved to better defeat those attempting to beat the system for malign ends.

SB almost certainly be suppressed. Banning it in one country would accomplish little except to hamper that nation’s technological development and economic growth. Certain types of research should be banned and some types of information restricted, however. The Biological and Toxins Weapons Convention (BWC), already in existence, provides a useful framework with which to begin assessing experiments of concern. The BWC currently commits the 162 nations that are parties to the convention to prohibit the development, production, and stockpiling of biological and toxin weapons. The absence of a formal verification regime to monitor compliance has limited the effectiveness of the BWC, with multilateral monitoring, verification, and sanctions established on a case by case basis through UN Security Council Resolutions and with sanctions imposed unilaterally by the United States and other powers when perceived interests are threatened. Over the long term, development of a formal regime under UN auspices to standardize monitoring, verification and sanctioning is of clear importance. In the near term, consortia of countries with significant concentrations of biotech production activity might spearhead a movement towards such restrictions.

Research

As described earlier, SB is likely to have significant defensive benefits. Although most experts we interviewed felt that near and medium-term offensive benefits are likely to be larger than defensive

ones, it is crucial to place this in the context of the current offense/defense balance. Given the current state of the technology, it is already vastly easier to attack than defend using biological weapons.¹²⁴ It is unclear that SB's further marginal contributions to offense will have a significant impact. Furthermore, interest in SB is well-established around the world, highlighted by the victory of teams from Slovenia and China in the 2006 and 2007 iGEM competitions. A restrictive approach to SB research is thus likely to be both fruitless and counterproductive. Instead, we suggest that security considerations stemming from the field be viewed through the lens of portfolio theory. In portfolio theory different uncorrelated risks can offset one another, allowing a portfolio of investments to have a lower total risk than any individual asset within it.^{125,126} In essence, any individual line of research in SB might well help potential attackers but pursuing many different research approaches, particularly if significant resources are devoted to those most likely to yield defensive benefits, should decrease total risk.

This approach is particularly mindful of the phenomenon Roger Brent dubbed "The Valley of the Shadow of Death," in which initial advances in biotechnology make attacks easier while later ones improve defensive capabilities enough to largely eliminate the threat from both natural and artificial pathogens.¹²⁷ Brent suggests that the best – indeed, the only – way in which to deal with this problem is to advance research in biotechnology as quickly as possible in the hope of moving through the Valley before a major attack occurs. Our analysis of the potential of SB strengthens the case for this approach. Significant investments in the promising defensive applications of SB may lessen absolute vulnerability by providing significant assets in warning and therapeutics production even in the medium term – making the Valley, in a sense, shallower. At the same time, SB's new set of techniques for genetic engineering may increase the speed of research, shortening the time until we reach Brent's theorized time of biological safety and metaphorically making the valley narrower.

Design

The last, and most ambitious, set of techniques for defusing SB's offensive potential revolve around the existence of a relatively small and cohesive community of synthetic biologists who, influenced by the study of previous technologies, are attempting to design the field's foundational technologies. For example, several major SB research projects seek to develop "chassis." These are basic architectures, usually derived from natural bacteria, which can be used as frameworks upon which particular SB applications can be installed, similar to the motherboard of a computer. Most chassis researchers intend to place their eventual designs in the public domain in order to encourage the growth of the field. Because of this, there is a significant possibility that the first few chassis designs, particularly if they perform relatively well, will be crucial to most SB applications for some time after they are released.

In designing chassis it may be possible to go beyond safety concerns. "Safe" chassis would be designed to be resistant to accidental changes in their function due to environmental effects or random mutation. Chassis designer should also, however, explore the possibility of designing chassis to be secure – resistant to deliberate change by synthetic biologists less-skilled or with fewer resources than their inventors. Chassis could, for example, have multiple interlinked controls which make them vulnerable to human immune systems and prevent them from multiplying at the temperature and pH (acidity) of the human body. In essence, this sort of research presents the opportunity to design a technology almost from the moment of its inception to limit its applicability to a targeted and specific subset of uses. The protective equivalent would be akin to chemists having the option to make it more difficult to use chemistry to make explosives, or computer scientists having designed programming languages so that viruses could not be written. This line of development is the most speculative of the approaches outlined here, but perhaps also the most promising. It affords the possibility of capturing all the potential benefits of SB with minimal consequences and suggests the possibility of an entirely new approach for dealing with technological risks. This approach is currently the subject of active research at SynBERC and seems

to have sufficient promise to merit continuing support over the long term. A targeted grant program would encourage younger investigators to direct part of their research toward this vital goal.

Conclusions

SB offers the potential for a revolution in the manipulation of living systems. At its best it might allow progress in biotechnology to approach the speed of that in information technology. Even far lower levels of success would offer significant benefits in fields ranging from medicine to industrial chemistry. As with any new technology, SB is likely to be a double-edged sword. Our analysis offers three basic findings on the effects of DNA synthesis and SB on offensive and defensive capabilities, categorized by time horizon:

- Over the short term (0-5 years) DNA synthesis and SB are unlikely to have significant offensive or defensive security implications. This lag provides time to develop policies to reduce medium-term offensive threats and to improve long-term defensive benefits, as noted below.
- Over the medium term (5-10 years), DNA synthesis and SB may foster development of pathways around conventional controls on natural agents and may enable development of some novel offensive capabilities. The security implications of these developments are unclear, as natural biological agents and conventional weapons are likely to continue to be more accessible and usable than biological agents produced using DNA synthesis and synthetic biology.
- Over the long term (10+ years), DNA synthesis and SB may strengthen defensive capabilities against biological attacks and responses to natural epidemics, as the methods of SB permit all of the defensive applications mentioned earlier, including: more rapid analysis of natural and artificial agents, accelerated design of vaccines and other pharmaceuticals appropriate to threats, and faster mass production of pharmaceuticals. SB may also foster the development of more discriminating, less lethal, or more controllable agents, or agents with characteristics entirely

absent from the natural world. Ironically, such advanced agents may have more utility than today's weapons of mass destruction, and hence may be more destabilizing.

This essay suggests a combination of policy approaches to mitigate potential harms from and maximize the potential benefits of synthetic biology, including community-based efforts, regulation and surveillance, further research, and the deliberate design of security and safety into the technology. These recommendations, however, must be paired with recognition of significant policy relevant uncertainty over the effects of SB on the diffusion of biological engineering capabilities, novel offensive and defensive capabilities, and norms, voluntary organizations, and mandatory controls on use.

Offensive capabilities are likely to diffuse more rapidly, and to more actors, than defensive ones, potentially undercutting the effectiveness of traditional policies that stress controls over materials and technologies. Furthermore, the modularized methods of SB may decrease the gradient between the capabilities of skilled and unskilled workers, as these methods reduce the value of the specialized craft knowledge of the advanced graduate students and postdoctoral fellows that now perform much of the shop-floor lifting in advanced biological engineering.

Although the trend toward diffusion of biotechnical capabilities seems clear, the rate and extent of diffusion cannot be projected with much confidence. The extent to which SB will in fact deliver on the promise of increased capabilities is one critical element of uncertainty. Synthetic biology is likely to increase the range of capabilities available to both attackers and defenders, decrease the resources necessary to launch an attack, and radically decrease the time required to generate new capabilities. Furthermore, it intensifies the possibility of "wild card" novel applications with implications that are difficult or impossible to characterize and analyze in advance. Although a basic trend toward enhanced capabilities of all types seems clear, specific predictions of augmented capabilities cannot be made with confidence. The extent to which SB will deliver on its promise to enable novel biological applications with shorter development times is a second critical element of uncertainty.

Synthetic biology may increase the potential utility of biological weapons, but the effects of this on norms and regulatory systems, as well as the impact of countervailing norms, community organizations, and regulatory controls, remain unknown. The development of novel applications and of defensive capabilities that limit the risk of blowback may increase the practical value of biological weapons and erode norms against their use. These possible effects on capabilities and norms may be offset, in whole or in part, by voluntary community-based responses and mandatory regulatory controls. The extent and effects of such efforts will depend in part on understandings and communications between the concerned research and technology communities, publics, and governmental agencies.

Our final suggestion centers on fostering adaptive responses to risks in light of these and other policy relevant sources of uncertainty. Respondents in our initial and follow-up surveys, commentators at conference presentations, and reviewers for this journal emphasized the existence of substantial uncertainty over the development of synthetic biology, its specific effects on security, and the effectiveness of responses to these effects, although there was substantial disagreement on the particular sources of this uncertainty.

When there is substantial uncertainty, the norms, rules, and procedures embodied in an international regime or domestic regulatory system will inevitably be wrong. If understandings of underlying causal structures are imperfect, then domestic and international regulatory systems based on those understandings will be flawed, because the knowledge needed to make informed decisions is lacking when they are created. Under such conditions, domestic regulations and international regimes should be viewed as experiments meant to generate information on political, economic, biological, or engineering assumptions that may in turn be used to update causal beliefs and policies. Properly designed regulatory systems harvest information generated by policy experience, and use that information to revise and update policies. Thus, the ultimate policy recommendation made here is to devise practical means to keep voluntary community based measures and mandatory regulatory controls yoked to an evolving knowledge base.¹²⁸

In conditions of uncertainty and change, as is the case for synthetic biology, individuals and organizations often adopt some form of trial-and-error operating philosophy. Most regulatory systems, however, do not act this way. The usual operating premise is that new standards and rules are to be regarded as valid in perpetuity. In our view, risk governance strategies for synthetic biology should be designed on the assumption that they must be updated and corrected as new information is acquired. In a handful of United States federal regulatory cases, planned adaptation of this sort does occur. The most instructive of those cases is the Environmental Protection Agency (EPA)'s National Ambient Air Quality Standards program for setting air quality standards for particulate matter (PM) in light of health effects information. The EPA has now conducted several iterations of such standard-setting, each time systematically reviewing the latest expert knowledge – which is now routinely abetted by a major EPA -- funded PM research effort - needed to improve air quality standards and incorporating that knowledge into new standards. This process has, over time, seen the redefinition of PM pollution from “total suspended solids” to one of special concern for very fine particles. A second prominent example is that of the post-marketing surveillance effort by the Food and Drug Administration (FDA). The point of this program is to understand and correct decisions about adverse health effects of new drugs based on information learned after the drugs are approved. The EPA and FDA cases appear to be solidly established and systematically accommodate new scientific and other knowledge into regularly-evolving decisions.¹²⁹

Risk governance in synthetic biology may be modeled after these self corrective EPA and FDA cases. Each of the specific recommendations above should be viewed as policy experiments. They are intended to accentuate benefits and minimize risks while also eliciting information on the nature of security and safety risks, the extent of economic, environmental, security and medical benefits, and the costs and the benefits of policies suggested. Such experiments will be most fruitful if their results are understood and accounted for by everyone affected by synthetic biology.

Tables

Table 1: Initial Interviews	
Interview	Subject Description
A	A founding figure of SB
B	SB with very high public profile
C	Director of one of the largest SB research initiatives
D	Path-breaking Synthetic Biologist and biomedical Engineer
E	Synthetic Biologist and Head of a SB professional organization
F	Leading figure in development of SB and DNA Synthesis
G	Senior consultant on biosecurity to Department of Homeland Security
H	Leader of a graduate program on biodefense

Table 2: Participation in International Genetically Engineered Machines Competition*			
Year	# of Teams	# of Participants	# of Countries
2004	5	50	1
2005	13	95	4
2006	38	400	15
2007	54	750	19
2008	84	1200	21

*Data from Randy Rettberg

Acknowledgements

The authors acknowledge with gratitude support from NSF for the Synthetic Biology Engineering Research Center (SynBERC) and for an MIT Integrative Research and Training Program on Assessing Implications and Improving Responses to Emerging Technologies and sabbatical research support, and to the Paul & Daisy Soros New American Foundation, which supported some of this research. The authors express their deep appreciation to the many leading practitioners of synthetic biology, experts on biological security issues, and staff of leading non-governmental organizations who generously volunteered their time to join in candid discussions with the authors of this study, and for their comments on the arguments and evidence presented in this essay; to panelists at SB 3.0 in Zurich in 2007 and participants in the International Risk Governance Council meeting on Governing Risks in Synthetic Biology in 2008 for engagement on these themes; and, to Dr. Rocco Casagrande for his detailed comments on an earlier draft of this manuscript. Responsibility for errors and omissions remains with the authors of this paper.

Gautam Mukunda is a PhD Candidate in the Massachusetts Institute of Technology's Department of Political Science. He is a Paul & Daisy Soros New American Fellow and an NSF IGERT Fellow. He is a graduate of Harvard College. His work has been published or is forthcoming in *Security Studies*, *Parameters*, and *Systems and Synthetic Biology*. His research interests include the role of leaders in foreign policy, innovation, particularly in militaries, and the social and political implications of synthetic biology.

Kenneth Oye, Ph.D., a political scientist, is an Associate Professor of Political Science and Engineering Systems at MIT. He has served on the faculties of the Harvard Kennedy School, the University of California, Princeton University, and Swarthmore College. He has written six books including *Cooperation Under Anarchy*, *Economic Discrimination and Political Exchange*, and *Eagle in a New World*. His current research interests involve using theory and methods from political economy to address issues in the field of science, technology, and environmental policy.

Scott C. Mohr, Ph.D., a chemist, is a Professor of Chemistry at Boston University, where he specializes in biophysical chemistry and bioinformatics. He serves as Professor of Graduate Studies for the Bioinformatics Program.

References

¹ Jonathan B. Tucker, 2002. A farewell to germs: The U.S. Renunciation of biological and toxin warfare, 1969-70. *International Security* 27 (1): 107-148.

² Mark Wheelis, 2003. A short history of biological warfare and weapons. In *The implementation of legally binding measures to strengthen the biological and toxin weapons convention*. M.I. Chevrier, K. Chomiczewski, M.R. Dando, H. Garrigue, G. Granaztoi and G.S. Pearson, Eds. Amsterdam: ISO Press, pp. 15-31.

³ Mark Wheelis, 2004. Chemical and biological terrorism: Lessons from history. In *International Seminar on Nuclear War and Planetary Emergencies, 31st Session: The Cultural Planetary Emergency*. R. Ragaini, Ed. Singapore: World Scientific Publishing, pp. 110-113.

-
- ⁴ Dany Shoham and Stuart M. Jacobsen, 2007. Technical intelligence in retrospect: The 2001 anthrax letters powder. *International Journal of Intelligence and Counterintelligence* 20 (1): 79-105.
- ⁵ ETC Group, 2007. Extreme genetic engineering: An introduction to synthetic biology.
- ⁶ Jonathan B. Tucker and Raymond A. Zilinskas, 2006. The promise and perils of synthetic biology. *The New Atlantis: A Journal of Technology & Society*: 25-45.
- ⁷ Richard Preston, 1997. *The cobra event*. New York, NY: Random House.
- ⁸ Committee on Research Standards and Practices to Prevent the Destructive Application of Biology, 2004. Biotechnology research in an age of terrorism. Washington: National Research Council of the National Academies.
- ⁹ Office of Transnational Issues, 2003. The darker bioweapons future. Central Intelligence Agency.
- ¹⁰ Jonathan B. Tucker, 2006. Preventing the misuse of biology: Lessons from the oversight of smallpox virus research. *International Security* 31 (2): 116-150.
- ¹¹ Mark Wheelis, 2002. Biotechnology and biochemical weapons. *Nonproliferation Review* 9 (1): 48-53.
- ¹² Mark Wheelis, 2004. Will the new biology lead to new weapons. *Arms Control Today* 34 (6): 6-13.
- ¹³ Kathryn Nixdorff, Neil Davison, Piers Millett and Simon Whitby, 2003. Technology and biological weapons: Future threats. In *Science and Technology Report*. College Park, MD: Center for International Security, Studies School of Public Affairs, University of Maryland.
- ¹⁴ Bob Graham, Jim Talent, Graham Allison, Robin Cleveland, Steve Rademajer, Tim Roemer, Wendy Sherman, Henry Sokolski and Rich Verma, 2008. World at risk: The report of the commission on the prevention of wmd proliferation and terrorism.
- ¹⁵ Anthony H. Cordesman, 2007. When to cry wolf, what to cry, and how to cry it. In *Bioterrorism: Confronting a complex threat*. Andreas Wenger and Reto Wollenmann, Eds. Boulder, CO: Lynne Rienner, pp. 155-178.
- ¹⁶ Malcolm Dando, Ibid. The impact of scientific and technological change. pp. 77-89.
- ¹⁷ Jeanne Guillemin, Ibid. The legacy of secret state programs. pp. 13-37.
- ¹⁸ Milton Leitenberg, Ibid. Evolution of the current threat. pp. 39-76.
- ¹⁹ Michele Garfinkel, Drew Endy, Gerald Epstein and Robert Friedman, 2007. Synthetic genomics: Options for governance. Alfred P. Sloan Foundation, p. 66.
- ²⁰ Hans Bügl, John P. Danner, Robert J. Molinari, John T. Mulligan, Han-Oh Park, Bas Reichert, David A. Roth, Ralf Wagner, Bruce Budowle, Robert M. Scripp, Jennifer A.L. Smith, Scott J. Steele, George Church and Drew Endy, 2007. DNA synthesis and biological security. *Nature Biotechnology* 25 (6): 627-629.
- ²¹ Jonathan B. Tucker and Raymond A. Zilinskas, 2006. The promise and perils of synthetic biology. *The New Atlantis: A Journal of Technology & Society*: 25-45.
- ²² Philip E. Tetlock, 2005. *Expert political judgment*. Princeton, NJ: Princeton University Press.
- ²³ Nassim Nicholas Taleb, 2007. *The black swan: The impact of the highly improbable*. New York, NY: Random House.
- ²⁴ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.
- ²⁵ Ibid.
- ²⁶ Jay Keasling, February 24, 2009. Overview of the center. NSF Site Visit, Berkeley, CA: SynBERC.
- ²⁷ Entrez Genome Project, Complete genomes. National Center for Biotechnology Information. Accessed: July 21, 2009. <http://www.ncbi.nlm.nih.gov/genomes/lproks.cgi>.
- ²⁸ Entrez Genome Project, Properties of eukaryotic genome sequencing projects. National Center for Biotechnology Information. Accessed: July 21, 2009. <http://www.ncbi.nlm.nih.gov/genomes/leuks.cgi>.

-
- ²⁹ National Center for Biotechnology Information, Genbank. National Institutes of Health. Accessed: July 21, 2009. <http://www.ncbi.nlm.nih.gov>.
- ³⁰ Growth of genbank, 2008. Accessed: July 23, 2009. <http://www.ncbi.nlm.nih.gov/Genbank/genbankstats.html>
- ³¹ National Center for Biotechnology Information, Genbank. National Institutes of Health. Accessed: July 21, 2009. <http://www.ncbi.nlm.nih.gov>.
- ³² Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.
- ³³ Michael B. Elowitz and Stanislas Leibler, 2000. A synthetic oscillatory network of transcriptional regulators. *Nature* 403: 335-338.
- ³⁴ Timothy S. Gardner, Charles R. Cantor and James J. Collins, Ibid. Construction of a genetic toggle switch in escherichia coli. 339-342.
- ³⁵ Thomas Knight, 2003. Idempotent vector design for standard assembly of biobricks. In *MIT Synthetic Biology Working Group*. Cambridge, MA: Massachusetts Institute of Technology.
- ³⁶ Rachel Wellhausen and Gautam Mukunda, 2009. The political economy of synthetic biology. *Systems and Synthetic Biology* 3 (Forthcoming).
- ³⁷ 2009. Synthetic biology: Scope, applications and implications. London, UK: The Royal Academy of Engineering.
- ³⁸ Rocco Casagrande, 2006. Homeland security 2015. In *Homeland Security 2015*. Washington, DC: Department of Homeland Security. This section draws heavily on the framework for the development of offensive bioweapons that Casagrande proposed in his article.
- ³⁹ Richard Preston, 2002. *The demon in the freezer*. New York, NY: Random House.
- ⁴⁰ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA, Richard Preston, 1994. *The hot zone*. New York, NY: Random House.
- ⁴¹ Rocco Casagrande, 2006. Homeland security 2015. In *Homeland Security 2015*. Washington, DC: Department of Homeland Security.
- ⁴² Neal A. Clinehens, 2000. Aum shinrikyo and weapons of mass destruction. Maxwell Air Force Base: Air Command and Staff College.
- ⁴³ John Sopko and Alan Edelman, 1995. Global proliferation of weapons of mass destruction: A case study on the aum shinrikyo.
- ⁴⁴ CDC national select agent registry select agent/toxin list, 2008. Accessed: July 22, 2009. <http://www.selectagents.gov/agentToxinList.htm>
- ⁴⁵ Terrence M. Tumpey, Christopher F. Basler, Patricia V. Aguilar, Hui Zeng, Alicia Solórzano, David E. Swayne, Nancy J. Cox, Jacqueline M. Katz, Jeffrey K. Taubenberger, Peter Palese and Adolfo García-Sastre, 2005. Characterization of the reconstructed 1918 spanish influenza pandemic virus. *Science* 310: 77-80.
- ⁴⁶ Robert Carlson, 2003. The pace and proliferation of biological technologies. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 1 (3).
- ⁴⁷ Michele Garfinkel, Drew Endy, Gerald Epstein and Robert Friedman, 2007. Synthetic genomics: Options for governance. Alfred P. Sloan Foundation, p. 66.
- ⁴⁸ Rocco Casagrande, 2006. Homeland security 2015. In *Homeland Security 2015*. Washington, DC: Department of Homeland Security.
- ⁴⁹ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.
- ⁵⁰ Ibid.

-
- ⁵¹ Jeronimo Cello, Aniko V. Paul and Eckard Wimmer, 2002. Chemical synthesis of poliovirus cDNA: Generation of infectious virus in the absence of natural template. *Science* 297: 1016-1018.
- ⁵² Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.
- ⁵³ Ibid.
- ⁵⁴ Gautam Mukunda and Scott Mohr, 2007. DNA synthesis, synthetic biology, and biosecurity. In *Synthetic Biology 3.0*. Zurich, Switzerland.
- ⁵⁵ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.
- ⁵⁶ Rocco Casagrande, 2006. Homeland security 2015. In *Homeland Security 2015*. Washington, DC: Department of Homeland Security.
- ⁵⁷ Ibid.
- ⁵⁸ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.
- ⁵⁹ Ibid.
- ⁶⁰ Rachel Nowak, 2001. Killer virus: An engineered mouse virus leaves us one step away from the ultimate bioweapon. In *New Scientist Online News*. Melbourne.
- ⁶¹ Wendy Orendt, 2004. A most dangerous game. In *Natural History*: FindArticles.com.
- ⁶² Nassim Nicholas Taleb, 2007. *The black swan: The impact of the highly improbable*. New York, NY: Random House.
- ⁶³ Testbeds, 2008. Accessed: February 21, 2009. <http://www.synberc.org/testbeds.html>
- ⁶⁴ M. Berdoy, J. P. Webster and D. W. Macdonald, 2000. Fatal attraction in rats infected with toxoplasma gondii. *Proceedings: Biological Sciences* 267 (1452): 1591-1594.
- ⁶⁵ Jonathan B. Tucker, 2002. A farewell to germs: The U.S. Renunciation of biological and toxin warfare, 1969-70. *International Security* 27 (1): 107-148.
- ⁶⁶ Robert Jervis, 1976. *Perception and misperception in international politics*. Princeton, NJ: Princeton University Press.
- ⁶⁷ Milton Leitenberg, James Leonard and Richard Spertzel, 2003. Biodefense crossing the line. *Politics and the Life Sciences* 22 (2): 2-3.
- ⁶⁸ Joseph A. DiMasi, Ronald W. Hansen and Henry G. Grabowski, 2003. The price of innovation: New estimates of drug development costs. *Journal of Health Economics* 22 (2): 151-185.
- ⁶⁹ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.
- ⁷⁰ Ibid.
- ⁷¹ Angelo DePalma, 2008. Vaccine development aided by new techniques. In *GEN: Genetic Engineering and Biotechnology News*.
- ⁷² G.T. Jennings and M.F. Bachmann, 2007. Designing recombinant vaccines with viral properties: A rational approach to more effective vaccines. *Current Molecular Medicine* 7: 143-155.
- ⁷³ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.
- ⁷⁴ Ibid.
- ⁷⁵ Ibid.
- ⁷⁶ M. Matthey and J. Spencer, 2008. Bacteriophage therapy - cooked goose or phoenix rising? *Current Opinion in Biotechnology* 19: 608-612.

-
- ⁷⁷ T. Rochat, L.G. Bermudez-Humaran, J.J. Gratadoux, C. Fourage, C. Hoebler, G. Corthier and P. Langella, 2007. Anti-inflammatory effects of lactobacillus casei bl23 producing or not a manganese-dependent catalase on dss-induced colitis in mice. *Microbial Cell Factories* 6 (22).
- ⁷⁸ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.
- ⁷⁹ Ibid.
- ⁸⁰ Kathleen Vogel, 2006. Bioweapons proliferation: Where science studies and public policy collide. *Social Studies of Science* 36 (5): 659-690.
- ⁸¹ Kathleen Vogel, 2008. Biodefense: Considering the sociotechnical dimension. In *Biosecurity interventions: Global health & security in question*. Andrew Lakoff and Stephen J. Collier, Eds. New York, NY: Columbia University Press, pp. 227-256.
- ⁸² David S. Landes, 1998. *The wealth and poverty of nations: Why some are so rich and some so poor*. New York, NY: W.W. Norton & Company. 278-9.
- ⁸³ Kathleen Vogel, 2006. Bioweapons proliferation: Where science studies and public policy collide. *Social Studies of Science* 36 (5): 659-690.
- ⁸⁴ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.
- ⁸⁵ Jay Keasling, February 24, 2009. Overview of the center. NSF Site Visit, Berkeley, CA: SynBERC.
- ⁸⁶ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.
- ⁸⁷ Ibid.
- ⁸⁸ Clayton M. Christensen and Michael E. Raynor, 2003. *The innovator's solution: Creating and sustaining successful growth*. Boston, MA: Harvard Business School Press.
- ⁸⁹ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.
- ⁹⁴ Details can be found at <http://sb4.biobricks.org/series/>.
- ⁹⁵ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.
- ⁹⁶ For example: Diybio, 2009. Accessed: July 21, 2009. <http://diybio.org/>
- ⁹⁷ Personal observations by the authors.
- ⁹⁸ Making a biological counter, 2008. Accessed: February 16, 2009. <http://io9.com/5049788/making-a-biological-counter>
- ⁹⁹ Greg Bear, 2007. *Quantico*. New York, NY: Vanguard Press.
- ¹⁰⁰ Tom Clancy, 1998. *Rainbow six*. New York, NY: Penguin Group.
- ¹⁰¹ Jessica Stern, 2002/03. Dreaded risks and the control of biological weapons. *International Security* 27 (3): 89-123.
- ¹⁰² 2004. An act to amend the public health service act to provide protections and countermeasures against chemical, radiological, or nuclear agents that may be used in a terrorist attack against the united states by giving the national institutes of health contracting flexibility, infrastructure improvements, and expediting the scientific peer review process, and streamlining the food and drug administration approval process of countermeasures. United States of America.
- ¹⁰³ Project bioshield: Progress in the war on terror, 2004. Accessed: August 28, 2007. <http://www.whitehouse.gov/infocus/bioshield/bioshield2.html>
- ¹⁰⁴ Lynne Gilfillan, Bradley T. Smith, Thomas V. Inglesby, Krishna Kodukula, Ari Schuler, Mark Lister and Tara O'Toole, 2004. Taking the measure of countermeasures: Leaders' views on the nation's capacity

to develop biodefense countermeasures. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 2 (4): 1-8.

¹⁰⁵ Kathleen Vogel, 2008. Biodefense: Considering the sociotechnical dimension. In *Biosecurity interventions: Global health & security in question*. Andrew Lakoff and Stephen J. Collier, Eds. New York, NY: Columbia University Press, pp. 227-256.

¹⁰⁶ Gregory Koblenz, 2003/04. Pathogens as weapons: The international security implications of biological warfare. *International Security* 28 (3): 84-122.

¹⁰⁷ Anthony H. Cordesman, 2002. Biological warfare and the buffy paradigm. In *CSIS Homeland Defense: Asymmetric Warfare & Terrorism*. Center for Strategic and International Studies.

¹⁰⁸ Peter R. Lavoy, 2007. Knowledge gaps and threat assessments. In *Bioterrorism: Confronting a complex threat*. Andreas Wenger and Reto Wollenmann, Eds. Boulder, CO: Lynne Rienner, pp. 93-118.

¹⁰⁹ Marie Isabelle Chevrier, *Ibid.* Why do conclusions from experts vary? , pp. 119-151.

¹¹⁰ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.

¹¹¹ Bob Graham, Jim Talent, Graham Allison, Robin Cleveland, Steve Rademajer, Tim Roemer, Wendy Sherman, Henry Sokolski and Rich Verma, 2008. World at risk: The report of the commission on the prevention of wmd proliferation and terrorism.

¹¹² Malcolm Dando, 2009. Biologists napping while work militarized. *Nature* 460 (7258): 950-951.

¹¹³ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.

¹¹⁴ Biowarfare for dummies, 2006. Accessed: February 16, 2009.

<http://www.kurzweilai.net/meme/frame.html?main=/articles/art0682.html>

¹¹⁵ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.

¹¹⁶ Claire M. Fraser and Malcolm R. Dando, 2001. Genomics and future biological weapons: The need for preventive action by the biomedical community. *Nature Genetics* 29: 253-256.

¹¹⁷ Brian Rappert, Marie Chevrier and Malcolm Dando, 2006. In-depth implementation of the btwc: Education and outreach. In *Bradford BTWC Review: Department of Peace Studies, Bradford University*.

¹¹⁸ Jeanne Guillemin, 2007. Can scientific codes of conduct deter bioweapons? *Audit of the Conventional Wisdom* (07-06): 1-4.

¹¹⁹ Aleksandra Mozdzanowska, 2005. Personal communication. Gautam Mukunda, Ed. Cambridge, MA.

¹²⁰ Hans Bügl, John P. Danner, Robert J. Molinari, John T. Mulligan, Han-Oh Park, Bas Reichert, David A. Roth, Ralf Wagner, Bruce Budowle, Robert M. Scripp, Jennifer A.L. Smith, Scott J. Steele, George Church and Drew Endy, 2007. DNA synthesis and biological security. *Nature Biotechnology* 25 (6): 627-629.

¹²¹ *Ibid.*

¹²² Michele Garfinkel, Drew Endy, Gerald Epstein and Robert Friedman, 2007. Synthetic genomics: Options for governance. Alfred P. Sloan Foundation, p. 66.

¹²³ Synthetic Biology and Biosecurity Experts, 2007. Interview. Scott Mohr and Gautam Mukunda, Eds. Cambridge, MA.

¹²⁴ Gregory Koblenz, 2003/04. Pathogens as weapons: The international security implications of biological warfare. *International Security* 28 (3): 84-122.

¹²⁵ Peter L. Bernstein, 1996. *Against the gods: The remarkable story of risk*. New York, NY: John Wiley & Sons.

¹²⁶ Peter L. Bernstein, 1992. *Capital ideas: The improbable origins of modern wall street*. New York, NY: The Free Press. 340.

¹²⁷ Roger Brent, 2005. *In the valley of the shadow of death*. Berkeley, CA: National Academy of Sciences.

¹²⁸ Lawrence McCray, Kenneth A. Oye and Arthur Petersen, 2009. Planned adaptation in risk regulation: A review of US environmental, health, and safety regulation. *Technology Forecasting and Social Change* 76 (Forthcoming).

¹²⁹ Ibid.