What rough beast?

Synthetic biology, uncertainty, and the future of biosecurity

Gautam Mukunda
Department of Political Science
Massachusetts Institute of Technology
77 Massachusetts Avenue, Room E53-470
Cambridge, MA 02139-4307
gautam.mukunda@gmail.com

Kenneth A. Oye
Engineering Systems Division
Department of Political Science
Massachusetts Institute of Technology
Cambridge, MA 02139-4307
oye@mit.edu

Scott C. Mohr
Department of Chemistry
Metcalf Center for Science and Engineering
Boston University
Boston, MA 02215-2521
mohr@bu.edu

ABSTRACT. **Synthetic biology 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 synthetic biology based on the insights of leading synthetic biologists into how the technology may develop, the projections of practicing biosecurity authorities on changes in the security context and potential security applications of synthetic biology, and joint appraisals of policy relevant sources of uncertainty. Synthetic biology appears to have minimal security implications in the near term, create modest offensive advantages in the medium term, and strengthen defensive capabilities against natural and engineered biological threats and enable novel potential offensive uses in the long term. To maximize defensive and minimize offensive effects of synthetic biology 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 features into the technology.**

Key words: synthetic biology, biosecurity, biodefense, biological weapons

> 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*

doi: 10.2990/28_2_2

After decades that have seen little 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 with them. Two religious cults attempted to cause mass casualties using biological weapons, but no deaths resulted from their attacks. Soon after the September 11 terrorist strikes, 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's Office of Transnational Issues, the National Research Council, and the National Science Advisory Board Recombinant DNA Advisory Committee are among many organizations that have directed attention in recent years 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 (also referred to as the Graham-Talent Commission after its chair and vice-chair) issued a 2008 report titled "World at Risk." 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 received particular attention. First, the basic tools of biological engineering have been developing rapidly, with exponential advances in productivity and declines in the 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 who call themselves synthetic biologists are using these tools to develop modularized approaches to the design and recombination of genetic materials. Practitioners of synthetic biology aspire to make genetic engineering easier, cheaper, more efficient, and more predictable, thereby accelerating the advance of biotechnology. If successful, synthetic biology 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 advance 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 synthetic biology on both defensive and offensive capabilities and recommends policies that may mitigate some of the security concerns which may arise. Our study is based on anonymous interviews with the most widely published and frequently cited practitioners of synthetic biology 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 the uncertainty associated with the development and application of synthetic biology and discuss ways that uncertainty may be addressed more effectively in policy.

This paper is organized into seven sections. First, we describe this study's methodology. Second, we offer a primer for non-biologists on the essentials of synthetic biology, with a discussion of how this emerging field differs from conventional genetic engineering. Third, we evaluate the contribution of synthetic biology to weapons production and offer a brief review of weapons development processes, with illustrations of how existing benign contributions from synthetic biology might be used in developing biological weapons. Fourth, we examine how synthetic biology 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, we analyze how synthetic biology's focus on decreasing

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

Table 1. Initial interviews.

Interview	*Subject description*
A	A founding figure of synthetic biology
B	Synthetic biologist with very high public profile
C	Director of one of the largest synthetic biology research initiatives
D	Path-breaking synthetic biologist and biomedical engineer
E	Head of a synthetic biology professional organization
F	Leading figure in development of synthetic biology and DNA synthesis
G	Senior consultant on biosecurity to Department of Homeland Security
H	Leader of a graduate program on biodefense

the skill necessary to modify biological systems and its emphasis on modular design may have security implications substantially beyond those normally attributed to advances in biotechnology. Sixth, we offer 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. Lastly, we summarize key conclusions on the near-term, medium-term, and long-term security implications of synthetic biology relative to offensive and defensive capabilities and make recommendations for designing policies that engage with the 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 regarding 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 their expertise in relevant fields, interest in issues involving the nexus between synthetic biology and biosecurity, and willingness to engage in a time-consuming interview process. We conducted eight initial interviews which averaged approximately 1.5 hours in length. The interview subjects are described in Table 1.

All interview subjects were promised anonymity to assure open and honest responses to questions on a highly controversial topic like biosecurity. Based on these interviews, we formulated tentative conclusions and policy recommendations. Third, we checked our initial conclusions with our original interview subjects and then consulted a wide variety of expert sources knowledgeable about synthetic biology and/or biosecurity. In this second round of interviews, we asked more narrowly focused questions of over 30 people with knowledge about particular aspects of synthetic biology and biosecurity and convened small group discussions on key 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 solicited feedback on preliminary versions of our analysis and conclusions through presentations at conferences, including the 2007 Synthetic Biology 3.0 meeting in Zurich, the 2008 International Risk Governance Council meeting on Governing Risks in Synthetic Biology, and the 2009 American Society of Microbiologists meeting on biodefense. At these meetings we met with many audience members both informally and in formal interviews.

Such an iterated, interview-based research design had several advantages. First, 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. Second, it allowed us to highlight key areas of disagreement and controversy within the synthetic biology and biosecurity communities by providing in-depth discussions over prolonged periods of time with researchers and policy actors representing a wide array of perspectives. Third, and perhaps most important, this approach allowed us to incorporate the ideas and views of experts in this emerging area on pivotal issues and points of disagreement. Key topics, ideas, and concepts were identified, discussed, and analyzed in depth, with evidence, 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 challenging. When modifications are made, 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. Synthetic biology shares with conventional genetic engineering the goal of developing practical applications ranging from the biosynthesis of pharmaceuticals, polymers, and fuels, to the detection and measurement of pollutants, drugs, and tumors, as well as the creation of controls that respond to light, temperature, and other signals. Synthetic biology differs from conventional 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 synthetic biology proceeds through three stages. First, it describes how DNA sequencing and systems biology provided the information that is now the foundation for synthetic biology. 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 thereafter, 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, along with 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 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]

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 they argued that much of the inspiration for synthetic biology came from the desire to engage in bioengineering in a way that did not require such an advanced level of understanding for its success.[32]

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

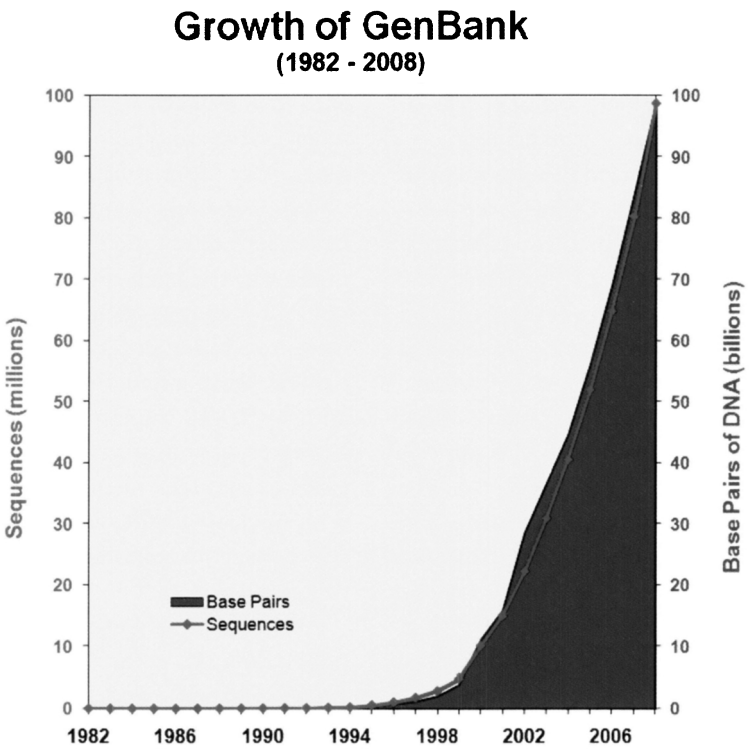

Figure 1. Growth of the publicly available gene-sequence database from its inception through 2008[30].

***Note*: As of mid-2009 the number of sequences had reached 106,073,709 containing 105,277,306,080 bases.[31] For the purpose of this illustration, a "base pair" is synonymous with a base.**

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 synthetic biology 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: first, 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, second, to use sets of genes to create novel engineered organisms with useful functions. The synthetic biology 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, synthetic biology is built around the concept of assembling useful devices from standardized components. The publication of two papers in the January 20, 2000 issue of *Nature* can, somewhat arbitrarily, be said to mark the beginning of modern synthetic biology.[33,34] The first paper, by a team from Princeton, 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

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

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, allowing 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. Researchers in this area have championed the principle of assembling useful complex devices from simple standardized genetic components as the core principle of synthetic biology. 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 synthetic biology devices will minimize major aspects of 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-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 they might also help improve defensive capabilities against both natural and artificial biological threats.

Potential effects on offense[38]

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.

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

The general advance of biotechnology, and especially the increased speed and lower cost of DNA synthesis, is likely to have implications for each of these processes. We focus, however, on the marginal impact of DNA synthesis and synthetic biology, 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 (i.e., 5 or more years), synthetic biology 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), synthetic biology 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 involves the acquisition of a suitable agent. Many such agents would be difficult or impossible even for states to acquire, and 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 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.[40,41] Even agents that seem easy to obtain can pose surprising difficulties. *Bacillua anthracis*, the bacterium that causes anthrax, is widely available in the natural world but most natural strains are not particularly dangerous.[42] 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.[43,44] 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 no longer existed in any form, either in the natural world or in storage.[45] 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.[46]

DNA synthesis technology is improving at exponential rates – faster, even, than Moore's Law which governs computer performance.[47] Such improvements may allow the acquisition of biological agents through synthesis, potentially broadening the pool of actors able to acquire such agents.[48] 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.[49] While virus genomes usually require little structural support to become active agents, a bacterial genome needs all of the other apparatus of a bacterial cell. Virtually all of 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.[50] 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.[51]

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-term (i.e., less than 10 years into the future) synthetic biology landscape. This is particularly likely given that the first to be artificially (re)constructed, the polio virus, was synthesized in 2002.[52] 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.[53]

Moving beyond DNA synthesis, however, synthetic biology techniques may further complicate the issues surrounding agent acquisition in the medium term (5 to 10 years) and, even more likely, long term (10 or more years). They may do so in two ways: by allowing the easier modification of natural agents, and by enabling

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

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 biological weapons using synthetic biology. Dual-use synthetic biology 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 could combine the qualities of several different organisms, each of which has some traits 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, perhaps eventually, bacterium.[54]

Creation of entirely synthetic agents – ones without natural analogues – although still some ways off, 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 initially, and several others in follow-up interviews, suggested that some of the already published work in synthetic biology presents systems that malicious actors might attempt to modify by straightforward procedures to produce potential bioweapons.[55] These efforts 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. After all, PCR (polymerase chain reaction), 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, absent that, "thousands of virus-free [chicken] eggs."[56] 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.[57] Advances in DNA synthesis and synthetic biology, however, are likely to have only second-order effects on this stage of production. 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 synthetic biology 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 stages of synthetic agent production are taken together, as the effects of synthetic biology 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 the munition and the agent 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.[58]

As with other stages of the weapons-manufacturing process, technical progress outside of DNA synthesis and synthetic biology is likely to continue to make weaponization easier as the skills and techniques involved spread beyond the weapons community.[59] 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, synthetic biology is likely to have only second-order effects. Synthetic biology might help potential attackers by allowing them to modify the

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

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.[60]

5. Effect

Synthetic biology is likely to have its largest impact in this stage, although it is unlikely to appear in the short or medium term. Natural pathogens suitable for biological attacks are characterized by their capacity 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 synthetic biology will be found in its ability to provide potential attackers with a much broader variety of potential new effects. These can be grouped 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.[61]

Perhaps the most significant aspect of this experiment was the unexpectedness of the results. Before these results were reported, most researchers had believed that modification of viruses would tend to make them less, not more, dangerous.[62] 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.[63] 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.

Synthetic biology 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 synthetic biology 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. Synthetic biology 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. Synthetic biology's emphasis on modularity creates the potential for sudden changes in the threat environment due to 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 synthetic biology, is seeking to develop tumor-killing bacteria as a potential early application of synthetic biology.[64] 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 synthetic biology, 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 synthetic biology 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 synthetic biology 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 synthetic biology components that produce sleep-inducing chemicals and *then* modifying the bacteria to make them capable of infecting subjects through the air. Combining such disparate discoveries would require 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 synthetic biology enterprise, if it succeeds, will make such combinations considerably easier. This example is only one of many such possible 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.[65] 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 or more years) proposition. All interviewed experts agreed, however, that if synthetic biology succeeds, it is highly likely, perhaps even almost certain, that it will be possible to construct such customized biological weapons.

This possibility has two significant secondary security implications. First, it is likely to significantly strengthen 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.[66] Advanced customized biological weapons, however, have the potential both to be more controllable than their unaltered counterparts and to give users capabilities they would 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. In a spiral dynamic the resources spent on *defense* by one state are interpreted as resources spent on *offense* by a second state. That second state increases its own defense spending in response, which the first state perceives as an increase in threat, causing it to increase its military spending once again. Both states can thus become trapped in an arms race and devote large resources to their militaries even though neither has any aggressive intentions.[67,68]

Implications for defense

Although the term "dual use" normally precedes a discussion of a technology's abusive applications, it also

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

implies positive ones. In the case of synthetic biology, 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 synthetic biology in these cases will depend on the degree to which it develops as a mature technology. Synthetic biology'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; indeed, this is one of the primary drivers behind the high cost to develop new drugs.[69] Despite this, all six of the synthetic biologists who were among our primary interviewees expressed great optimism about synthetic biology's potential to eventually make significant contributions to such defensive uses, and several noted that it has already begun to help with the production of validated molecules. In follow-up interviews, respondents sometimes expressed some doubt as to how soon synthetic biology 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.[70] This difference may have been an artifact of respondents in the secondary interviews being generally less senior than those in the first round.

Improved surveillance

Surveillance to detect pathogenic agents in a population takes two basic forms: (1) classical epidemiological analysis of the distribution and symptoms of the victims of infectious disease (supplemented by syndromic surveillance techniques,) and (2) 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. Synthetic biology 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 can also 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 in international competitions. 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.[71]

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.[72] DNA vaccine technology could be enhanced by synthetic biology 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 bioweapons, 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.[73] Synthetic biology techniques provide an ideal toolbox to accomplish this goal. Engineered adjuvants – chemicals added to a vaccine to magnify the immune response it provokes – might also be generated more effectively using synthetic biology techniques.[74]

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

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 or mass production. Pharmaceutical companies developing antibiotics must also deal with the waste created by the generation of side products in a chemical synthesis.[75]

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 stereoisomers of the desired compound. Stereoisomers are molecules with the correct formula but a mirror-image geometry that renders them biologically inert. Conventional chemical production is usually a multistage process during which 50 percent 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. Synthetic biology may enable much easier use of engineered enzymes in the production of complex organic molecules, eliminating the waste due to stereoisomer 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 synthetic biology techniques, if a new type of organism were to be identified for which no available antibiotic is effective, metabolic engineering via synthetic biology 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 synthetic biology will eventually afford is likely to be a significant advantage to defenders against biological attacks and, of course, natural diseases as well.

Biodefense via 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 cancer therapies as well as in biodefense.[76]

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.[77] A report on the protective effect of a strain of *Lactobacillus casei* against chemically induced ulcerative colitis (an inflammatory bowel disease) in mice provides a prototype example for possible roles of engineered bacteria as potential therapeutic agents.[78]

The SynBERC testbed aimed at engineering bacterial cells to target tumors and inject toxins to kill the cancer cells that make them up 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 steps, but they nevertheless justify optimism that synthetic biology could lead to an era where powerful defensive tools can be developed much more rapidly than now.[79]

Implications of deskilling and diffusion

Every initial interviewee who worked specifically on synthetic biology suggested that one of its most important aspects is the deskilling of biological engineering combined with the creation of techniques to alter living systems using modular design. This was

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

unanimously affirmed by other synthetic biologists in follow-up interviews.[80] 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 consists of procedural and substantive knowledge primarily gained from experience instead of formal education, which in biology is usually acquired through prolonged apprenticeships with senior scientists. This is common practice within both academic and commercial biotechnology circles. Interestingly, 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.[81,82]

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.[83] The American factories simply lacked the tacit knowledge not conveyed in the blueprints. Today, however, all that a sophisticated factory equipped with automated processes and facilities for modular designs would need is an e-mailed CAD file. In a similar way, the normal progress of biotechnology may "replace or...alter the kind of tacit knowledge required for bioweapons development."[84] 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, commented "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."[85]

SynBERC in particular has focused upon the elimination of tacit knowledge from the manipulation of living systems. The center structures its research around a hierarchy of standardized biological parts, devices, and chassis, which are meant to allow for the easy creation of biological systems with artificial properties. SynBERC 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."[86] The emphasis here is crucial. SynBERC certainly seeks to produce various specific applications but that is not its primary goal. Instead the center 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 assembly of DNA segments, while others are developing software for the computer-aided design of living systems.[87] Although these and other such attempts may initially fail, or succeed only in part, they mark a crucial and fundamental divide between synthetic biology and traditional bioengineering. Synthetic biology includes, as a principal part of its agenda, a sustained, well-funded assault on the necessity of tacit knowledge in bioengineering and thus on one of the most important current barriers to the production of biological weapons.

This deskilling is complementary with synthetic biology'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 unexpected 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, a project by Amyris Biotechnology to produce artemisinin commercially in yeast using synthetic biology techniques involved the alteration of 16 genes.[88]

Synthetic biology attempts to eliminate these interaction effects by creating standardized modular biological parts that are meant to be insulated from 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.[89,90] Nonetheless, if these efforts bear fruit they will make the alteration of biological systems vastly faster and less expensive to accomplish,

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

an effect that is magnified by the combination of deskilling and modularity.

These two processes are thus likely to have effects beyond those already specified. Synthetic biology is likely to eventually 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. Deskilling and modularity, however, have the potential to both rapidly increase the diffusion of skills and decrease the skill gradient separating elite practitioners from non-experts. Diffusion of new biotechnologies will increase because the investment in time and resources needed 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. By contrast, the high degree of tacit knowledge involved in traditional genetic engineering means that less-skilled practitioners can have significant difficulty replicating the achievements of the most-skilled members of their field, even if all the necessary data has been published. In the case of synthetic biology, deskilling and modularity are likely to make replication of such achievements vastly easier, substantially leveling the gradient between elite and peripheral practitioners.

Another important dimension to consider entails efforts by synthetic biologists to encourage internationalization. Of the first four annual conferences devoted to synthetic biology, two were held outside the United States, one in Zurich and the other in Hong Kong.[91] Another growing activity has been the International Genetically Engineered Machines (iGEM) competition, which involves undergraduate and graduate student teams in synthetic biology projects. Thousands of students from more than 20 different countries involving nearly 100 colleges and universities have been initiated into the procedures of synthetic biology, developing a baseline competence while 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 doctoral graduates and post-doctoral fellows who have trained in synthetic biology 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.

Table 2. Participation in the International Genetically Engineered Machines competition*.

Year	*Number of teams*	*Number of participants*	*Number of countries*
2004	5	50	1
2005	13	95	4
2006	38	400	15
2007	54	750	19
2008	84	1200	21
2009	112	1700	26

*Data from Randy Rettberg

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 synthetic biology community on this point, with some 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.[92] Much like the now-legendary pioneers of the personal computer revolution, amateur synthetic biologists are beginning to wax enthusiastic about conducting synthetic biology experiments at home. Do-It-Yourself Biology (almost always referred to by its acronym, DIYB) has recently become quite popular, especially as evidenced by online websites dedicated to the topic.[93] Although there is currently no evidence of any malicious intent by those 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 do-it-yourself biologists operate at a fairly simple level and often display naiveté about many molecular biology laboratory basics.[94] 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 outfit a home laboratory with all of the key pieces of equipment for performing synthetic biology experiments by buying from used equipment dealers, or simply eBay. Katherine Aull, for example, a recent

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

graduate of MIT, entered the "Mad Science Contest" sponsored by io9.com, 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.[95] Notably, her design uses the genetic toggle switch described earlier in this paper as one of its key components, which illustrates 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, the more ambitions their agenda might become. At present it remains a stretch to imagine that some of the more lurid, as yet fictional possibilities might be realized.[96,97] 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, if not overreactions, to potential threats.[98] 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.[99,100,101,102] 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.[103] 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.[104,105,106]

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, we will examine 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.[107,108] The most important medium-term offensive impact of synthetic biology is likely to be its potential to lower the level of skill necessary to acquire or synthesize an agent. The combination of deskilling 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 synthetic biology's offensive potential and maximize its contribution to biodefense. Malcolm Dando, a prominent British expert on biological weapons, has argued that life scientists in general are "alarming[ly]" disengaged with the potential security implications of their discoveries.[109] The synthetic biology community, however, is a notable exception to this trend. The major annual synthetic biology 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 synthetic biology, combined with the heightened interest in biosecurity since the anthrax attacks of October 2001, has led to a wide array of innovative approaches to maximizing synthetic biology's contribution to biosecurity. These approaches can be divided into four categories: community, regulation/surveillance, research, and design. Each of these approaches revolves around the idea of increasing the obstacles and resources necessary to craft a bioweapon using synthetic biology 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. But by making the task more difficult, they can eliminate the threat from less capable actors and push back the time by which even more capable actors will have access to the full panoply of modalities offered by the new science, thereby

buying time for potential beneficial applications in the hands of defensive-minded governments.

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 on the continued development of the technology itself. This could well be true even if the actual harm was negligible, as is most likely to be the case from any such incident.[110] 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 synthetic biology curriculum as it develops.

Community

Interview subject B suggested that the creation of a synthetic biology 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 with other interview subjects, he described several potential advantages that such an institution could bring. Among these are the inculcation of norms against working on bioweapons; the provision of alternative means of support for scientists who are assigned tasks which they find ethically questionable; the fostering of stronger community bonds that could help provide alerts about possible offensive programs; and, the establishment and enforcement of community codes of conduct.

Several synthetic biologists and experts who focus primarily on traditional biosecurity recommended specific 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 mutual support and open communication. Insofar as possible, he recommended developing bottom-up efforts to educate and socialize laboratory scientists in synthetic biology. 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, for example, that discuss how easy it might be to build a bioweapon, as illustrated by Paul Boutin's piece "Biowar for Dummies."[111]

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.[112] Although we agree that the United States government's current posture vastly over-emphasizes the need for secrecy, 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 and all biodefense research should be conducted as openly as possible, with an emphasis on ensuring that scientists from close allies are included. 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 that a community organization could help solve.[113,114] 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.[115] Relying on such organizations as a primary or principal means of defense against the offensive use of these technologies could actually 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 nontrivial benefits at negligible cost.

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

We also recommend the adoption of a "safety hold" norm similar to that 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.[116] Developing such a norm in the synthetic biology 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 synthetic biology 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 synthetic biology 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 synthetic biology 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." [117] This would include the requirement that those ordering synthesized DNA must verify their identity and that companies use approved screening software to ensure compliance with all regulations.[118] Similarly, the Sloan Foundation funded a wide-reaching study to assess the security implications of DNA synthesis, which highlighted the importance of screening orders among a larger list of procedures to improve safety and security.[119]

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 synthetic biology community.[120] 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 synthetic biology are characterized by a "hacking" culture. Instead of attempting to suppress this inventive input, there are ways in which hackers might be enlisted 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 share the results, allowing the software to be improved to better defeat those attempting to beat the system for malign ends.

Looking to the future, synthetic biology research should not be suppressed. An outright ban in one country would accomplish little except to hamper that nation's technological development and economic growth. Certain *types* of research might be banned and information restricted, however. The international 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 thus far limited the effectiveness of the BWC, with multilateral monitoring, verification, and sanctions established on a case by case basis through UN Security Council Resolutions. Sanctions are also 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 of synthetic biology production 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, synthetic biology 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.[121] It is unclear that synthetic biology's further marginal contributions to offense will have a significant impact. Furthermore, interest in synthetic biology 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 synthetic biology 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.[122,123] Although any individual line of synthetic biology research might potentially assist attackers, the pursuit of 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 substantially eliminate the threat from both natural and artificial pathogens.[124] Brent suggests that the best – indeed, the only – effective way 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 synthetic biology strengthens the case for this approach. Significant investments in the promising defensive applications of synthetic biology may lessen absolute vulnerability by improving warning systems and providing significant assets in therapeutics production even in the medium term, making the Valley, in a sense, shallower. At the same time, synthetic biology's new set of techniques for genetic engineering may *increase* the speed of research, shortening the time it takes to reach Brent's theorized point of biological safety and metaphorically making the Valley narrower.

Design

The last, and most ambitious, set of techniques for defusing synthetic biology'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 research projects seek to develop safer chassis-like components. These are basic architectures, usually derived from natural bacteria, which can be used as frameworks upon which particular synthetic biology applications can be installed, similar to the motherboard of a computer. Most chassis researchers intend to place their eventual designs in the public domain 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 synthetic biology 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 designers should also explore the possibility of designing chassis to be secure, that is, resistant to deliberate change by less-skilled synthetic biologists or those 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 the most promising, for it affords the possibility of capturing all the potential benefits of synthetic biology with minimal consequences and suggests the possibility of

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

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

Synthetic biology 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 information technology development. Even modest gains would offer significant benefits in fields ranging from medicine to industrial chemistry. As with any new technology, synthetic biology is likely to be a double-edged sword. Our analysis offers three basic findings on the effects of DNA synthesis and synthetic biology on offensive and defensive capabilities, categorized by time horizon:

- Over the short term (0 to 5 years), DNA synthesis and synthetic biology are unlikely to have significant offensive or defensive security implications. This lag provides time to develop policies to reduce medium-term offensive threats and improve long-term defensive benefits, as noted below.
- Over the medium term (5 to 10 years), DNA synthesis and synthetic biology 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 remain more accessible and usable than biological agents produced using DNA synthesis and synthetic biology.
- Over the long term (10 or more years), DNA synthesis and synthetic biology may strengthen defensive capabilities against biological attacks and responses to natural epidemics, as the methods of synthetic biology permit all of the defensive applications mentioned earlier, including more rapid analysis of natural and artificial agents, accelerated design of vaccines and pharmaceuticals, and faster mass production of pharmaceuticals. Synthetic biology 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.

Our analysis 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 integration of security and safety design features into the technology. These recommendations, however, must be paired with recognition of significant policy relevant uncertainty over the effects of synthetic biology on the diffusion of biological engineering innovations, novel offensive and defensive capabilities, and the norms, voluntary standards, and mandatory controls on use.

Offensive capabilities are likely to diffuse more rapidly, and to more actors, than defensive capabilities, potentially undercutting the effectiveness of traditional policies that stress controls over materials and technologies. Furthermore, the modularized methods of synthetic biology 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 synthetic biology 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 unanticipated "wild card" applications with consequences 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 synthetic biology will deliver on its promise to

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

enable novel biological applications with shorter development times is thus 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, particularly when combined with the potential creation of countervailing norms, community organizations, and regulatory controls, cannot be predicted with any degree of certainty or precision. The development of novel applications and defensive capabilities that limit the risk of blowback may increase the practical value of biological weapons and erode norms against their use. These influences on the capabilities of synthetic agents and the norms governing their use may be offset, in whole or in part, by a combination of 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 research and technology communities, concerned 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 disagreement on the particular sources of this uncertainty.

When substantial uncertainty exists, the norms, rules, and procedures embodied in an international regime or domestic regulatory system will inevitably be flawed. If understandings of underlying causal structures are imperfect, then domestic and international regulatory systems based on those understandings will reflect this patchiness, because the knowledge needed to make informed decisions will be lacking. Under such conditions, domestic regulations and international regimes should be viewed as experiments meant to generate information relevant to 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 utilize 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.[125]

Under conditions of uncertainty and change, 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 becomes available. In a handful of 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 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 research effort, needed to improve air quality standards and incorporating that knowledge into new standards. Over time, this process has seen the redefinition of particulate matter 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 acquired after the drugs are approved. The EPA and FDA cases appear to be solidly established and systematically accommodate new scientific findings and other knowledge into regularly evolving decisions.[126]

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 suggested policies. Such experiments will be most fruitful if their results are understood and accounted for by the widest possible community of synthetic biology stakeholders.

https://doi.org/10.2990/28_2_2 Published online by Cambridge University Press

Note

The authors acknowledge with gratitude support from NSF for the Synthetic Biology Engineering Research Center (Grant #050869) and for an MIT Integrative Research and Training Program award on Assessing Implications and Improving Responses to Emerging Technologies (Grant #0333010) as well as sabbatical research support, and to the Paul & Daisy Soros New American Fellowship, which also 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 Synthetic Biology 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. Thanks also to Tara Maller, Josh Shifrinson, Phil Haun, and Peter Krause for their comments and suggestions. Responsibility for errors and omissions remains with the authors of this paper.

Gautam Mukunda is a Ph.D. 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 University, after which he was a consultant with McKinsey & Company focusing in the pharmaceutical sector. 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., is an Associate Professor of Political Science and Engineering Systems at MIT. He directs the MIT Program on Emerging Technologies (PoET) and is a faculty investigator in NSF SynBERC. 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., is a Professor of Chemistry at Boston University, where he specializes in biophysical chemistry and bioinformatics. He is a graduate of Williams College, *summa cum laude*, and received his Ph.D. from Harvard University. He is a member of Sigma Xi and has been an NIH Postdoctoral Fellow, Danforth Fellow, and NSF Fellow. Among other journals, his work has been published in *Science*, *Molecular Phylogenetics and Evolution*, and *Genome Biology*. He serves as Director of Graduate Studies for Boston University's Bioinformatics Program.

References

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

2. Mark Wheelis, "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, 2003), pp. 15–31.

3. Mark Wheelis, "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, 2004), pp. 110–113.

4. Dany Shoham and Stuart M. Jacobsen, "Technical intelligence in retrospect: The 2001 anthrax letters powder," *International Journal of Intelligence and Counterintelligence*, 2007, 20 (1): 79–105.

5. Etc Group, "Extreme genetic engineering: An introduction to synthetic biology," 2007.

6. Jonathan B. Tucker and Raymond A. Zilinskas, "The promise and perils of synthetic biology," *The New Atlantis: A Journal of Technology & Society*, Spring 2006: 25–45.

7. Richard Preston, *The Cobra Event* (New York: Random House, 1997).

8. Committee on Research Standards and Practices to Prevent the Destructive Application of Biology, *Biotechnology Research in an Age of Terrorism* (Washington, DC: National Research Council of the National Academies, 2004).

9. Office of Transnational Issues, "The darker bioweapons future" (Langley, VA: Central Intelligence Agency, 2003).

10. Jonathan B. Tucker, "Preventing the misuse of biology: Lessons from the oversight of smallpox virus research," *International Security*, Fall 2006, 31 (2): 116–150.

11. Mark Wheelis, "Biotechnology and biochemical weapons," *Nonproliferation Review*, Spring 2002, 9 (1): 48–53.

12. Mark Wheelis, "Will the new biology lead to new weapons," *Arms Control Today*, July/August 2004, 34 (6): 6–13.

13. Kathryn Nixdorff, Neil Davison, Piers Millett, and Simon Whitby, "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, 2003).

14. Bob Graham, Jim Talent, Graham Allison, Robin Cleveland, Steve Rademajer, Tim Roemer, Wendy Sherman, Henry Sokolski, and Rich Verma, *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism* (New York: Vintage Books, 2008).

15. Anthony H. Cordesman, "When to cry wolf, what to cry, and how to cry it," in *Bioterrorism: Confronting a Complex Threat*, A. Wenger and R. Wollenmann, eds. (Boulder: Lynne Rienner, 2007), 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, *Synthetic Genomics: Options for Governance* (New York: Alfred P. Sloan Foundation, 2007), 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, "DNA synthesis and biological security," *Nature Biotechnology*, June 2007, 25 (6): 627–629.

21. Jonathan B. Tucker and Raymond A. Zilinskas, "The promise and perils of synthetic biology," *The New Atlantis: A Journal of Technology & Society*, Spring 2006: 25–45.

22. Philip E. Tetlock, *Expert Political Judgment* (Princeton: Princeton University Press, 2005).

23. Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2007).

24. *Synthetic biology and biosecurity expert interviews*, 2007. Scott Mohr and Gautam Mukunda, eds. Cambridge, MA.

25. Ibid.

26. Jay Keasling, Overview of the center. NSF Site Visit, Berkeley, CA: SynBERC, February 24, 2009.

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. Mohr and Mukunda, Interviews.

33. Michael B. Elowitz and Stanislas Leibler, "A synthetic oscillatory network of transcriptional regulators," *Nature*, January 20 2000, 403: 335–338.

34. Timothy S. Gardner, Charles R. Cantor, and James J. Collins, "Construction of a genetic toggle switch in escherichia coli," *Ibid.*: 339–342.

35. Thomas Knight, "Idempotent vector design for standard assembly of biobricks," in *MIT Synthetic Biology Working Group* (Cambridge, MA: Massachusetts Institute of Technology, 2003).

36. Rachel Wellhausen and Gautam Mukunda, "Aspects of the political economy of development and synthetic biology," *Systems and Synthetic Biology*, December 2009, 3 (1–4): 115–123.

37. *Synthetic Biology: Scope, Applications and Implications* (London: The Royal Academy of Engineering, 2009).

38. Rocco Casagrande, "Homeland security 2015," in *Homeland Security 2015* (Washington, DC: Department of Homeland Security, 2006). This section draws heavily on the framework for the development of offensive bioweapons that Casagrande proposed in his article.

39. Richard Preston, *The Demon in the Freezer* (New York: Random House, 2002).

40. Mohr and Mukunda, Interviews.

41. Richard Preston, *The Hot Zone* (New York: Random House, 1994).

42. Casagrande, "Homeland security 2015."

43. Neal A. Clinehens, *Aum Shinrikyo and Weapons of Mass Destruction* (Maxwell Air Force Base, AL: Air Command and Staff College, 2000).

44. John Sopko and Alan Edelman, "Global proliferation of weapons of mass destruction: A case study on the Aum Shinrikyo," Staff statement in *Global Proliferation of Weapons of Mass Destruction*; in Hearings, Permanent Subcommittee on Investigation, Committee on Governmental Affairs (Washington, DC: United States Senate, Part I, 1996), pp. 47–102.

45. CDC national select agent registry select agent/toxin list, 2008. Accessed July 22, 2009, http://www.selectagents.gov/agentToxinList.htm

46. 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, "Characterization of the reconstructed 1918 Spanish influenza pandemic virus," *Science*, 7 October 2005, 310: 77–80.

47. Robert Carlson, "The pace and proliferation of biological technologies," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, 2003, 1 (3).

48. Garfinkel et al., p. 66.

49. Casagrande, "Homeland security 2015."

50. Mohr and Mukunda, Interviews.

51. Ibid.

52. Jeronimo Cello, Aniko V. Paul and Eckard Wimmer, "Chemical synthesis of poliovirus cDNA: Generation of infectious virus in the absence of natural template," *Science*, 9 August 2002, 297: 1016–1018.

53. Mohr and Mukunda, Interviews.

54. Ibid.

55. Gautam Mukunda and Scott Mohr, "DNA synthesis, synthetic biology, and biosecurity," in *The proceedings of Synthetic Biology 3.0* (Zurich, Switzerland, 2007).

56. Mohr and Mukunda, Interviews.

57. Casagrande, "Homeland security 2015."

58. Ibid.

59. Mohr and Mukunda, Interviews.

60. Ibid.

61. Rachel Nowak, "Killer virus: An engineered mouse virus leaves us one step away from the ultimate bioweapon," *New Scientist Online News* (Melbourne, Australia, 2001).

62. Wendy Orendt, "A most dangerous game," *Natural History*: FindArticles.com (2004).

63. Taleb.

64. Testbeds, 2008. Accessed February 21, 2009. http://www.synberc.org/testbeds.html

65. M. Berdoy, J. P. Webster, and D. W. Macdonald, "Fatal attraction in rats infected with toxoplasma gondii," *Proceedings: Biological Sciences*, 2000, 267 (1452): 1591–1594.

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

67. Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976).

68. Milton Leitenberg, James Leonard, and Richard Spertzel, "Biodefense crossing the line," *Politics and the Life Sciences*, September 2003, 22 (2): 2–3.

69. Joseph A. Dimasi, Ronald W. Hansen and Henry G. Grabowski, "The price of innovation: New estimates of drug development costs," *Journal of Health Economics*, March 2003, 22 (2): 151–185.

70. Mohr and Mukunda, Interviews.

71. Ibid.

72. Angelo Depalma, "Vaccine development aided by new techniques," *GEN: Genetic Engineering and Biotechnology News*, November 1, 2008. Accessed November 17, 2009, http://www.genengnews.com/articles/chitem.aspx?aid=2651

73. G.T. Jennings and M.F. Bachmann, "Designing recombinant vaccines with viral properties: A rational approach to more effective vaccines," *Current Molecular Medicine*, 2007, 7: 143–155.

74. Mohr and Mukunda, Interviews.

75. Ibid.

76. Ibid.

77. M. Mattey and J. Spencer, "Bacteriophage therapy: Cooked goose or phoenix rising?" *Current Opinion in Biotechnology*, 2008, 19: 608–612.

78. T. Rochat, L.G. Bermudez-Humaran, J.J. Gratadoux, C. Fourage, C. Hoebler, G. Corthier and P. Langella, "Anti-inflammatory effects of lactobacillus casei bl23 producing or not a maganese-dependent catalase on dss-induced colitis in mice," *Microbial Cell Factories*, 2007, 6 (22).

79. Mohr and Mukunda, Interviews.

80. Ibid.

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

82. Kathleen Vogel, "Biodefense: Considering the sociotechnical dimension," in *Biosecurity interventions: Global Health and Security in Question*, A. Lakoff and S. J. Collier, eds. (New York: Columbia University Press, 2008), pp. 227–256.

83. David S. Landes, *The Wealth and Poverty of Nations: Why Some Are So Rich and Some So Poor* (New York: W.W. Norton & Company, 1998), pp. 278–279.

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

85. Mohr and Mukunda, Interviews.

86. Keasling.

87. Mohr and Mukunda, Interviews.

88. Ibid.

89. Clayton M. Christensen and Michael E. Raynor, *The Innovator's Solution: Creating and Sustaining Successful Growth* (Boston: Harvard Business School Press, 2003).

90. Mohr and Mukunda, Interviews.

91. Details can be found at http://sb4.biobricks.org/series/.

92. Mohr and Mukunda, Interviews.

93. For example, DIYbio, 2009. Accessed July 21, 2009, http://diybio.org/

94. Personal observations by the authors.

95. Making a biological counter, 2008. Accessed February 16, 2009, http://io9.com/5049788/making-a-biological-counter

96. Greg Bear, *Quantico* (New York: Vanguard Press, 2007).

97. Tom Clancy, *Rainbow Six* (New York: Penguin Group, 1998).

98. Jessica Stern, "Dreaded risks and the control of biological weapons," *International Security*, Winter 2002/03, 27 (3): 89–123.

99. Project Bioshield Act of 2004, 118 STAT.835. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ276.108.pdf

100. Project bioshield: Progress in the war on terror, 2004. Accessed August 28, 2007, http://www.whitehouse.gov/infocus/bioshield/bioshield2.html

101. Lynne Gilfillan, Bradley T. Smith, Thomas V. Inglesby, Krishna Kodukula, Ari Schuler, Mark Lister, and Tara O'Toole, "Taking the measure of countermeasures: Leaders' views on the nation's capacity to develop biodefense countermeasures," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, October 12 2004, 2 (4): 1–8.

102. Kathleen Vogel, "Biodefense: Considering the sociotechnical dimension," in *Biosecurity Interventions: Global Health and Security in Question*, A. Lakoff and S. J. Collier, eds. (New York: Columbia University Press, 2008), pp. 227–256.

103. Gregory Koblentz, "Pathogens as weapons: The international security implications of biological warfare," *International Security*, Winter 2003/04, 28 (3): 84–122.

104. Anthony H. Cordesman, "Biological warfare and the Buffy paradigm," in *CSIS Homeland Defense: Asymmetric Warfare and Terrorism* (Washington, DC: Center for Strategic and International Studies, 2001).

105. Peter R. Lavoy, "Knowledge gaps and threat assessments," in *Bioterrorism: Confronting a Complex Threat*, Andreas Wenger and Reto Wollenmann, eds. (Boulder, CO: Lynne Rienner, 2007), pp. 93–118.

106. Marie Isabelle Chevrier, Ibid. "Why do conclusions from experts vary?" pp. 119–151.

107. Mohr and Mukunda, Interviews.

108. Graham et al.

109. Malcolm Dando, "Biologists napping while work militarized," *Nature*, August 20, 2009, 460 (7258): 950–951.

110. Mohr and Mukunda, Interviews.

111. Biowarfare for dummies, 2006. Accessed February 16, 2009, http://www.kurzweilai.net/meme/frame.html?main=/articles/art0682.html

112. Mohr and Mukunda, Interviews.

113. Claire M. Fraser and Malcolm R. Dando, "Genomics and future biological weapons: The need for preventive action by the biomedical community," *Nature Genetics*, 22 October 2001, 29: 253–256.

114. Brian Rappert, Marie Chevrier, and Malcolm Dando, "In-depth implementation of the BTWC: Education and outreach," in *Bradford BTWC Review* (Department of Peace Studies, University of Bradford, Bradford, UK, 2006).

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

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

117. 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, "DNA synthesis and biological security," *Nature Biotechnology*, June 2007, 25 (6): 627–629.

118. Ibid.

119. Garfinkel et al., p. 66.

120. Mohr and Mukunda, Interviews.

121. Gregory Koblentz, "Pathogens as weapons: The international security implications of biological warfare," *International Security*, Winter 2003/04, 28 (3): 84–122.

122. Peter L. Bernstein, *Against the Gods: The Remarkable Story of Risk* (New York: John Wiley & Sons, 1996).

123. Peter L. Bernstein, *Capital Ideas: The Improbable Origins of Modern Wall Street* (New York: The Free Press, 1992), p. 340.

124. Roger Brent, *In the Valley of the Shadow of Death* (Berkeley, CA: National Academy of Sciences, 2005). Accessed November 17, 2009, dspace.mit.edu/bitstream/handle/1721.1/34914/Valley2006.pdf?...

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

126. Ibid.