

This PDF is available at <http://nap.edu/24832>

SHARE    



## A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology: Interim Report

### DETAILS

51 pages | 8.5 x 11 | PAPERBACK  
ISBN 978-0-309-46283-9 | DOI 10.17226/24832

### CONTRIBUTORS

Committee on Strategies for Identifying and Addressing Biodefense Vulnerabilities Posed by Synthetic Biology; Board on Chemical Sciences and Technology; Board on Life Sciences; Division on Earth and Life Studies; National Academies of Sciences, Engineering, and Medicine

GET THIS BOOK

FIND RELATED TITLES

Visit the National Academies Press at [NAP.edu](http://NAP.edu) and login or register to get:

- Access to free PDF downloads of thousands of scientific reports
- 10% off the price of print titles
- Email or social media notifications of new titles related to your interests
- Special offers and discounts



Distribution, posting, or copying of this PDF is strictly prohibited without written permission of the National Academies Press. (Request Permission) Unless otherwise indicated, all materials in this PDF are copyrighted by the National Academy of Sciences.

Copyright © National Academy of Sciences. All rights reserved.

***A PROPOSED FRAMEWORK FOR  
IDENTIFYING POTENTIAL BIODEFENSE  
VULNERABILITIES POSED BY SYNTHETIC BIOLOGY:  
INTERIM REPORT***

Committee on Strategies for Identifying and Addressing Biodefense  
Vulnerabilities Posed by Synthetic Biology

Board on Chemical Sciences and Technology

Board on Life Sciences

Division on Earth and Life Studies

*This prepublication version of A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology: Interim Report has been provided to the public to facilitate timely access to the Consensus Study Report. Although the substance of the report is final, editorial changes may be made throughout the text and citations will be checked prior to publication. The final report will be available through the National Academies Press in summer 2017.*

A Consensus Study Report of  
*The National Academies of*  
**SCIENCES • ENGINEERING • MEDICINE**

THE NATIONAL ACADEMIES PRESS

Washington, DC

[www.nap.edu](http://www.nap.edu)

**PREPUBLICATION COPY: UNCORRECTED PROOFS**

Copyright National Academy of Sciences. All rights reserved.

**THE NATIONAL ACADEMIES PRESS 500 Fifth Street, NW Washington, DC 20001**

This project was supported by Contract No. HQ0034-16-C-0062 between the National Academy of Sciences and the U.S. Department of Defense. Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the view of any organization or agency that provided support for the project.

Digital Object Identifier: <https://doi.org/10.17226/24832>

Copyright 2017 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America

Suggested citation: National Academies of Sciences, Engineering, and Medicine. 2017. *A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology: Interim Report*. Washington, DC: The National Academies Press. doi: <https://doi.org/10.17226/24832>.

**PREPUBLICATION COPY: UNCORRECTED PROOFS**

*The National Academies of*  
**SCIENCES • ENGINEERING • MEDICINE**

The **National Academy of Sciences** was established in 1863 by an Act of Congress, signed by President Lincoln, as a private, nongovernmental institution to advise the nation on issues related to science and technology. Members are elected by their peers for outstanding contributions to research. Dr. Marcia McNutt is president.

The **National Academy of Engineering** was established in 1964 under the charter of the National Academy of Sciences to bring the practices of engineering to advising the nation. Members are elected by their peers for extraordinary contributions to engineering. Dr. C. D. Mote, Jr., is president.

The **National Academy of Medicine** (formerly the Institute of Medicine) was established in 1970 under the charter of the National Academy of Sciences to advise the nation on medical and health issues. Members are elected by their peers for distinguished contributions to medicine and health. Dr. Victor J. Dzau is president.

The three Academies work together as the **National Academies of Sciences, Engineering, and Medicine** to provide independent, objective analysis and advice to the nation and conduct other activities to solve complex problems and inform public policy decisions. The National Academies also encourage education and research, recognize outstanding contributions to knowledge, and increase public understanding in matters of science, engineering, and medicine.

Learn more about the National Academies of Sciences, Engineering, and Medicine at [www.nationalacademies.org](http://www.nationalacademies.org).

**PREPUBLICATION COPY: UNCORRECTED PROOFS**

*The National Academies of*  
**SCIENCES • ENGINEERING • MEDICINE**

**Consensus Study Reports** published by the National Academies of Sciences, Engineering, and Medicine document the evidence-based consensus on the study's statement of task by an authoring committee of experts. Reports typically include findings, conclusions, and recommendations based on information gathered by the committee and the committee's deliberations. Each report has been subjected to a rigorous and independent peer-review process and it represents the position of the National Academies on the statement of task.

**Proceedings** published by the National Academies of Sciences, Engineering, and Medicine chronicle the presentations and discussions at a workshop, symposium, or other event convened by the National Academies. The statements and opinions contained in proceedings are those of the participants and are not endorsed by other participants, the planning committee, or the National Academies.

For information about other products and activities of the National Academies, please visit [www.nationalacademies.org/about/whatwedo](http://www.nationalacademies.org/about/whatwedo).

**PREPUBLICATION COPY: UNCORRECTED PROOFS**

**COMMITTEE ON STRATEGIES FOR IDENTIFYING AND ADDRESSING  
BIODEFENSE VULNERABILITIES POSED BY SYNTHETIC BIOLOGY**

*Members*

**MICHAEL IMPERIALE** (*Chair*), University of Michigan Medical School  
**PATRICK BOYLE**, Ginkgo Bioworks  
**PETER A. CARR**, Massachusetts Institute of Technology Lincoln Laboratory  
**DOUGLAS DENSMORE**, Boston University  
**DIANE DIEULIIS**, National Defense University  
**ANDREW ELLINGTON**, The University of Texas at Austin  
**GIGI KWIK GRONVALL**, Johns Hopkins Center for Health Security  
**CHARLES HAAS**, Drexel University  
**JOSEPH KANABROCKI**, The University of Chicago  
**KARA MORGAN**, Battelle Memorial Institute  
**KRISTALA JONES PRATHER**, Massachusetts Institute of Technology  
**THOMAS SLEZAK**, Lawrence Livermore National Laboratory  
**JILL TAYLOR**, Wadsworth Center

*Staff*

**MARILEE SHELTON-DAVENPORT**, Study Director  
**KATHERINE BOWMAN**, Senior Program Officer  
**JO HUSBANDS**, Scholar/Senior Project Director  
**JENNA OGILVIE**, Research Associate  
**JARRETT NGUYEN**, Senior Program Assistant

*Sponsor*

**U.S. DEPARTMENT OF DEFENSE**

NOTE: See Section on Disclosure of Conflict of Interest.

## Acknowledgment of Reviewers

This Consensus Study Report was reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise. The purpose of this independent review is to provide candid and critical comments that will assist the National Academies of Sciences, Engineering, and Medicine in making each published report as sound as possible and to ensure that it meets the institutional standards for quality, objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process.

We thank the following individuals for their review of this report:

**HARVEY BLANCH**, University of California, Berkeley

**JAMES DIGGANS**, Twist Bioscience

**JAY D. KEASLING**, University of California, Berkeley

**DAVID WALT**, Tufts University

**NANCY D. CONNELL**, Rutgers University

**KAREN E. NELSON**, J. Craig Venter Institute (JCVI)

**GARY ACKERMAN**, University of Maryland

**ANITA JONES**, University of Virginia

**PIERS MILLET**, Future of Humanity Institute

**GERALD PARKER**, Texas A&M College of Veterinary Medicine and Biomedical Sciences

**HENRY WILLIS**, The RAND Corporation

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations of this report nor did they see the final draft before its release. The review of this report was overseen by Michael Ladisch of Purdue University. He was responsible for making certain that an independent examination of this report was carried out in accordance with the standards of the National Academies and that all review comments were carefully considered. Responsibility for the final content rests entirely with the authoring committee and the National Academies.

## Contents

<b>SUMMARY</b> .....	1
<b>INTRODUCTION</b> .....	1
<b>THE COMMITTEE’S PROCESS</b> .....	3
<b>STUDY SCOPE AND DEFINITIONS</b> .....	4
Biotechnology and Synthetic Biology, 4	
Synthetic Biology in the Context of Biodefense, 5	
Terminology, 6	
<b>FRAMEWORK APPROACH</b> .....	6
Approach to Developing the Framework, 6	
Uses and Limitations of the Framework, 8	
Parameters to Consider, 9	
<b>ROWS IN THE FRAMEWORK:</b>	
<b>TECHNOLOGIES AND APPLICATIONS TO ASSESS</b> .....	10
Design, 12	
Build, 16	
Test, 20	
<b>COLUMNS IN THE FRAMEWORK: FACTORS FOR ASSESSING CONCERN</b> .....	21
Factors to Assess Capability for Malicious Use, 22	
Factors to Assess Capability for Mitigation, 31	
<b>CONCLUSION</b> .....	34
<b>REFERENCES</b> .....	35
<b>COMMITTEE BIOGRAPHIES</b> .....	39
<b>DISCLOSURE OF CONFLICT OF INTEREST</b> .....	44



## SUMMARY

Building on an increasingly sophisticated understanding of naturally occurring biological processes, researchers have developed technologies to predictably modify or create organisms or biological components. This research, known collectively as synthetic biology, is being pursued for a variety of purposes, from reducing the burden of disease to improving agricultural yields to remediating pollution. While synthetic biology is being pursued primarily for beneficial and legitimate purposes, it is possible to imagine malicious uses that could threaten human health or military readiness and performance. Making informed decisions about how to address such concerns requires a comprehensive, realistic assessment. To this end, the U.S. Department of Defense, working with other agencies involved in biodefense, asked the National Academies of Sciences, Engineering, and Medicine to develop a framework to guide an assessment of the security concerns related to advances in synthetic biology, to assess the level of concern warranted for various advances and identify areas of vulnerability, and to prioritize options to address these vulnerabilities.

This interim report proposes a framework for identifying and prioritizing potential areas of concern associated with synthetic biology—a tool to aid the consideration of concerns related to synthetic biology. The framework describes categories of synthetic biology technologies and applications—such as genome editing, directed evolution, and automated biological design—and provides a set of initial questions to guide the assessment of concern related to these technologies and applications. These include questions about the technologies themselves, questions about potential actor use, and questions about the ability to create a weapon. The framework also outlines factors to assess capability for mitigation. In its final report, the committee will refine the framework as needed and use the parameters outlined to provide the U.S. Department of Defense with a detailed assessment of the concerns presented by these technologies and applications, as well as options for mitigation.

## INTRODUCTION

Scientific advances over the past several decades have rapidly accelerated the ability to engineer existing living organisms and potentially create novel ones not found in nature. Technologies to modify or create organisms or biological components—activities known collectively as synthetic biology—are being pursued for a variety of purposes, from reducing the burden of disease to improving agricultural yields to remediating pollution (see Box 1). These technologies are being developed and refined by researchers in universities, governments, and industry in the United States and around the globe. While biotechnology is being pursued primarily for beneficial and legitimate purposes, there are potential uses that are detrimental to humans, other species, and ecosystems. In order to inform investments to mitigate the threats, those responsible for protecting the security of nations must consider how these emerging technologies might be used in acts of warfare or terrorism, the intent and capability of adversaries to effect such uses, and the potential impacts of such attacks.

Statements and reports issued over the past several years have come to different conclusions regarding the national security threats posed by emerging biotechnologies and the level of concern that is warranted. Former Director of National Intelligence James Clapper, in his annual threat assessment to Congress, grouped concerns about genome editing, an example of synthetic biology technology, under discussion of weapons of mass destruction (Clapper 2016). Reports of federal government advisory committees, such as the report produced by the President’s Council of Advisors on Science and Technology in November 2016 on “Action Needed to Protect against Biological Attack” (PCAST 2016)

and a report produced by the JASON advisory group in 2016 on potential implications of CRISPR and other technologies on U.S. national security (Breaker 2017), similarly identify that biotechnology presents a new and significant threat. However, bioweapons are not a new phenomenon, and others have countered that, although advances in synthetic biology may add to the biological weapons landscape, these developments do not fundamentally change the landscape or warrant special action to address concerns (Vogel 2013; Jefferson et al. 2014). That argument is based on the notion that using natural pathogens to cause harm may be easier and just as effective as using synthetic biology to create bioweapons, so synthetic biology does not change the level of concern, at least not yet (A. Paul interview with K. Vogel, February 24, 2006, New York as cited in Vogel 2012; Jefferson et al. 2014).

### **BOX 1: Benefits of Synthetic Biology**

The field of synthetic biology opens tremendous possibilities for the application of biotechnology to improve human well-being, as well as the health of animals, plants, and the environment. Such applications hold substantial economic potential. For example, annual U.S. revenues from genetically engineered plants and microbes are estimated to exceed \$300 billion, and industrial biotechnology (the use of biological components to generate industrial products) is estimated to account for more than \$115 billion in annual U.S. revenues. New applications for biotechnology, particularly those driven by innovation in synthetic biology, are expected to further grow the size and reach of the bioeconomy (White House 2012).

Often looked to as a means of producing products that would otherwise be difficult to obtain, synthetic biology has already led to new ways of producing pharmaceuticals including opioids and the anti-malarial drug artemisinin. There are significant ongoing efforts to engineer microorganisms to produce fuels, act as detection devices, and clean up toxic spills. Synthetic biology is also seen as a potential means to grow organs for transplant, manipulate the microbiome, and even produce cosmetics. In addition to such application-driven goals, synthetic biology is also advancing the reach and role of science in society by inspiring more people to engage in biological experimentation, such as through the International Genetically Engineered Machine (iGEM) competition or by engaging with community laboratories. This broad array of applications and implications suggests that the potential benefits of synthetic biology are limited only by human creativity and imagination.

While it is possible to imagine numerous types of malicious uses that could be achieved with synthetic biology, making informed decisions about whether and how to mitigate these potential uses requires a comprehensive, realistic assessment of the security concerns this technology creates. To that end, the U.S. Department of Defense, working with other agencies involved in biodefense, asked the National Academies to develop a framework to guide an assessment of the security concerns related to advances in synthetic biology, to assess the level of concern warranted for various advances and identify areas of vulnerability, and to prioritize options to address these vulnerabilities. The committee's Statement of Task is presented in Box 2.

### **BOX 2: Statement of Task**

To assist the U.S. Department of Defense's Chemical and Biological Defense Program (CBDP), the National Academies of Sciences, Engineering, and Medicine will appoint an ad hoc committee to address the changing nature of the biodefense threat in the age of synthetic biology. Specifically, the focus of the study will be the manipulation of biological functions, systems, or microorganisms resulting in the production of disease-causing agents or toxins. The study will be conducted in two primary phases. Initially, the committee will develop a strategic framework to guide an assessment of the potential security vulnerabilities related to advances in biology and biotechnology, with a particular emphasis on synthetic biology.

The framework will focus on how to address the following three questions: What are the possible security concerns with regard to synthetic biology that are on the horizon? What are the time frames of development of these concerns? What are our options for mitigating these potential concerns? The committee will publish a brief interim, public report outlining the developed framework. This framework will not be a threat assessment, but rather, will focus on ways to identify scientific developments to enable opportunities that have the potential to mitigate threats posed by synthetic biology in the near-, mid-, and long-term, with the specific time frames defined by the committee. The framework will lay out how best to consider the trajectory of scientific advances, identify potential areas of vulnerability, and predict promising mitigation opportunities.

In Phase 2 of the study, the committee will use the outlined strategic framework to generate an assessment of vulnerabilities posed by synthetic biology. Inputs to this assessment may include information about the current threat, current program priorities and research, and an evaluation of the current landscape of science and technology. Conclusions and recommendations will include a list and description of vulnerabilities posed by synthetic biology and prioritized options to address them.

### **THE COMMITTEE'S PROCESS**

To carry out its charge, the National Academies appointed a committee of experts. Members provide the perspectives of academia, industry, government, and the nonprofit sector and have experience in synthetic biology, biosafety, microbiology, public health, bioinformatics, and risk assessment. In Phase 1 of the study, the committee met two times in person, held two webinars featuring three speakers, and convened many times via phone to gather information, understand the needs of the relevant federal agencies, and develop a framework to guide the study's second phase.

The committee began by reviewing existing frameworks related to biodefense and to synthetic biology, as well as previous assessments and other work related to synthetic biology and other biotechnology threats (NRC 2004; IOM/NRC 2006; IAC/IAP 2012; Tucker 2012; U.S. Government 2012, 2014; HHS 2013; Cummings and Kuzma 2017; DiEuliis and Giordano 2017). The committee then defined what type of framework would best guide an assessment of concerns related to synthetic biology, identified major categories of relevant technologies and applications to assess, and refined the factors to include in the assessment. The framework presented in this interim (Phase 1) report is the outcome of those deliberations.

In Phase 2 of the study, the committee will solicit comments on the framework from the synthetic biology research community and other relevant stakeholders. After refining the framework as needed, the committee will gather additional data during open committee sessions and assess each factor

as it applies to the technologies and applications under consideration. The outcome of the study's second phase will be an assessment of the concerns related to synthetic biology with recommendations on how the U.S. Department of Defense might address areas of greatest concern.

The committee did not leverage classified information that others have created in their consideration of related questions. Classified information was not included in the committee's deliberations; the resulting report is not classified and can be shared publicly. This facilitates the involvement of the wider community of synthetic biology subject-matter experts in the discussions that ensue during the committee's deliberations and after the committee's reports are produced.

## **STUDY SCOPE AND DEFINITIONS**

The study's sponsor is the U.S. Department of Defense's Chemical and Biological Defense Program, a program focused largely on protecting the warfighter against chemical and biological threats. However, the committee's work is not solely focused on the warfighter. In order to aid decision making in agencies across the biodefense enterprise, including the U.S. Department of Homeland Security, the U.S. Department of Health and Human Services' Office of the Assistant Secretary for Preparedness and Response, the intelligence community, and other agencies, the U.S. Department of Defense asked the committee to consider potential concerns that are relevant to all U.S. citizens, both at home and abroad, in both civilian and military contexts.

The following sections describe the committee's use of key terminology and outline what is within—and what is outside of—the committee's Phase 1 task.

### **Biotechnology and Synthetic Biology**

Biotechnology is a broad term encompassing the application of biological components or processes to advance human purposes. Although the term itself is thought to have been in use for only about a century, humans have used various forms of biotechnology for millennia. Synthetic biology refers to a set of methods within biotechnology that emerged much more recently, since around the year 2000. The two papers that are often referenced as establishing synthetic biology as its own field are by Elowitz and Leibler (2000) and Gardner et al. (2000). Although there remains no universally agreed-upon definition of synthetic biology (with some defining it more narrowly and others more broadly), perhaps the simplest distillation is that synthetic biology “aims to improve the process of genetic engineering” (Voigt 2012). Although genetic engineering was occurring—and improving—prior to 2000, that year marked a shift toward the adoption of approaches common to other engineering disciplines, but which had been previously given only modest attention in genetic engineering. These include the curation of standardized parts for building biological systems, the intensive use of models and other quantitative tools to simulate biological designs before building them, and the use of iterative Design-Build-Test (DBT) cycles to continuously improve these approaches. Key developments exemplifying these approaches include the establishment of standardized genetic parts registries, open-source DNA assembly methods, and rationally designed genetic circuits (Elowitz and Leibler 2000; Gardner et al. 2000; Knight 2003; Parts.igem.org 2017). In the committee's view, it is the adoption and global dissemination of these methods and tools to accelerate the engineering of living organisms that marked the transition to the age of synthetic biology.

Synthetic biology is enabled by tools and techniques from a variety of scientific disciplines from electrical engineering to computation to biology to chemistry. For example, the exponential improvements in DNA sequencing capabilities, initially developed to further our understanding of the human genome but soon applied to characterize many other organisms, have provided crucial raw material for synthetic biology and fueled innovation over the past decade. More recently, emerging genome editing tools such as CRISPR/Cas9 (Jinek et al. 2012; Cong et al. 2013) have been adopted for synthetic biology techniques such as the regulation of gene circuits and the development of gene drives (Esvelt et al. 2014). Scientific progress in domains relevant to synthetic biology has been remarkably rapid; CRISPR/Cas9, for example, was extended from mammalian cell culture (in the United States) to primates (in China) in a single year (Cong et al. 2013; Jinek et al. 2013; Mali et al. 2013; Niu et al. 2014). Instead of drawing sharp distinctions between advances in biotechnology and advances in synthetic biology, the committee believes it is reasonable to assume that the synthetic biology toolkit will continue to advance and be integrated into all biotechnology and biological research activities.

### **Synthetic Biology in the Context of Biodefense**

In its Phase 1 activities, the committee was tasked with developing a tool or process for assessing the biodefense threat in the age of synthetic biology. While the committee avoided rigidly defining synthetic biology, its deliberations were guided by the biodefense-relevant aspects of synthetic biology as outlined in the study's Statement of Task, namely "the manipulation of biological functions, systems, or microorganisms resulting in the production of a disease-causing agent or toxin." Modifying a pathogen to facilitate its rapid spread through a population, manipulating a biological system to produce a potent toxin, introducing antibiotic resistance into an infectious microorganism, or purposely weakening a person's immune system are just a few examples of the potential types of malicious uses of synthetic biology the committee considered under this guidance.

There are other conceivable uses of synthetic biology that, while arguably important to national security, are outside the scope of this study. The study focuses on activities that could directly threaten human health or the capacity of military personnel to execute their missions. The committee did not address the potential ways in which plants, animals, and the pathogens that affect them could be modified for malicious purposes, for example, to undermine agricultural productivity, although the economic and societal impact of such an attack could be substantial. The committee also did not address the modification of organisms to affect the environment or materials, except insofar as such efforts would directly impact warfighters by, for example, degrading their protective gear. Nonetheless, the technologies that might be used to threaten agricultural, environmental, or material targets, and the capabilities associated with those technologies, are likely comparable or even identical to the technologies and capabilities included in the committee's framework; as a result, the framework may be useful for a broader array of contexts than those addressed in this study.

It was also out of the committee's purview to weigh the benefits on balance with the risks of synthetic biology advancements. The committee acknowledges the tremendous value of synthetic biology to a number of societal goals but made no attempt to compare the size or nature of those benefits with the potential risks. It is not the intent of the committee or study sponsor to in any way imply that research efforts that use synthetic biology approaches should be curtailed.

## Terminology

The committee made deliberate decisions about the use of terminology to appropriately reflect the scope and nature of its work. The committee uses *agent* or *bioagent* broadly to refer to any product created using biological components that may be intended to cause harm. In the context of synthetic biology, an agent could be a pathogen, a toxin, or even a biological component, such as a genetic construct or a biochemical pathway that may be developed with the intent to harm a human target. *Capability* refers to the ability for an actor to produce and use an agent (or in some contexts, the ability for a target to mitigate adverse outcomes).

*Vulnerability* refers to potentially malicious capabilities against which we are not currently well protected. The committee did not formally assess vulnerability in its Phase 1 activities but will do so in Phase 2. The committee uses *degree of concern* in reference to the intensity of the experts' opinion regarding potential misuse. *Threat* and *risk* are terms with specific meanings in the context of defense and risk assessment that make them inappropriate for use in reference to the committee's Phase 1 activities. In the context of defense, threat encompasses both an actor's capability and the actor's intent. The committee was asked to examine capabilities but not the intent of actors, and did not have access to intelligence regarding what actors may be attempting to do, or who those actors are. As a result, the study does not provide a threat assessment per se, but rather offers a framework for considering the types of malicious actions that could conceivably be taken and assessing the degree of concern that might be warranted. The term risk refers to the likelihood and severity of harm. Again, because the intent of actors is not being considered, the likelihood of the harm cannot be fully estimated, so the term risk is not used in reference to the committee's own framework at this stage.

## FRAMEWORK APPROACH

The goal of developing a framework in Phase 1 of this study is to provide a basis for identifying and prioritizing potential areas of concern associated with synthetic biology. In its Phase 2 activities, the committee will use the framework, presented in Figure 1, in three main ways: (1) to analyze specific applications of synthetic biology, (2) to identify current areas of concern created by synthetic biology, and (3) to identify future potential areas of concern created by synthetic biology. After the committee's Phase 2 report is published, others may use the framework in all of these ways and, in addition, may find the framework useful for assessing the significance of new biotechnology developments that occur in the future.

### Approach to Developing the Framework

The committee drew from a substantial amount of existing work related to the question of how to assess security concerns, and this framework is intended to build upon that work, not replace it. A number of frameworks have been developed to assess concerns associated with emerging technologies (IOM/NRC 2006; Tucker 2012). In biology, these frameworks have typically been used to assess concern based on the features and capabilities of the biotechnology itself, specifically the capabilities the technology may provide to an actor who would wish to pursue a particular malicious use. In addition, some existing frameworks are designed to facilitate consideration of the severity of potential adverse outcomes and the ability to approach them through tools for detection, mitigation, or attribution.

Design	Build	Test	Synthetic Biology Technologies and Applications	Factors to Assess Capability for Malicious Use			Factors to Assess Capability for Mitigation				
				Use of Technology	Use as a Weapon	Attributes of Actors	Deterrence and Prevention Capabilities	Capability to Recognize an Attack	Attribution Capabilities	Consequence Management Capabilities	
■	■	■	Automated Biological Design								
			Metabolic Engineering								
			Phenotype Engineering								
			Horizontal Transfer and Transmissibility								
			Xenobiology								
			Human Modulation								
	■	■	■	DNA Construction							
				Editing of Genes or Genomes							
				Library Construction							
				Booting of Engineered Constructs							
				High-Throughput Screening							
				Directed Evolution							

**FIGURE 1 Committee’s Proposed Framework.** Committee’s proposed framework with factors to consider presented as columns. Synthetic biology technologies and applications to consider are presented as rows. Shading shows which phases of the Design-Test-Build cycle the synthetic biology technologies align with most closely.

Additional work has focused on assessing concern associated with particular types of experimentation; some elements of these frameworks can also be applicable to a broader set of concerns about technologies with potential beneficial and harmful uses. In the realm of security, scenario-based frameworks are commonly used to assess concerns and consider potential mitigation options. However, the committee determined that open-ended “red-teaming” approaches are not as helpful for an analysis

of concerns related to synthetic biology for three reasons: (1) there is a lack of real-life examples to provide an adequate evidence base, (2) it is possible to imagine an almost limitless number of potential malevolent uses for synthetic biology, and (3) it is difficult to draw generalized and actionable conclusions solely from scenario-based analyses.

The committee met with representatives of the U.S. Department of Defense in a public session to clarify the committee's understanding of the Statement of Task. Recognizing the committee members' high level of expertise in synthetic biology and related areas, the study sponsor emphasized that what was needed from the committee was a tool or process that could be used to determine how much concern any identified use of synthetic biology could pose, the time frame in which the potential use could become feasible given the expected rate of technological advancement, and information about potential mitigation options. In developing the framework, the committee understood "concern" to capture the degree to which the committee believes a hypothetical use of synthetic biology could realistically be achievable and lead to a negative impact for which the U.S. Department of Defense may want to prepare. Furthermore, because biotechnology changes so rapidly, the committee determined that it would be ideal for the framework to be developed in a way that allows it to be applied to assess technologies that emerge in the future and allows it to be updated as science and technology advance.

Figure 2 outlines the DBT concept and categories of synthetic biology technologies and applications (rows) that the committee deemed important to consider given its charge. In its Phase 1 deliberations, the committee participated in a consensus process to develop and refine the framework. In its Phase 2 deliberations, the committee will expand on this work by using the framework to conduct an analysis of the technologies and applications identified in its Phase 1 report, as well as any additional potential applications identified through feedback on the Phase 1 report. This second phase will include an analysis of the specific factors (columns) and refinement of the questions identified in the framework rows, as well as an assessment of the current level of concern for each factor, the timeframes to be considered, and consideration of uncertainty.

### **Uses and Limitations of the Framework**

The committee designed its framework as a tool to aid the consideration of concerns related to biotechnology and synthetic biology. It is intended to be flexible enough to be applied in a variety of circumstances and for a variety of purposes, such as: analyzing existing biotechnologies to evaluate the level of concern warranted at present; understanding how various technologies or capabilities compare to, interact with, or complement each other in terms of their level of concern; identifying key bottlenecks and barriers that, if removed, could lead to a change in the level of concern; evaluating the change in the level of concern warranted when new experimental results are reported or new technologies arise; and horizon scanning to predict or prepare for potential future areas of concern. In these ways, the framework can be used to facilitate both reactive analysis (related to developments that have already occurred) and proactive analysis (related to predicting future developments).

While the framework can serve many purposes, it also has some important limitations. As noted previously, assessing information on actors' intent is outside of the scope of this committee's activities. As such, factors related to assessing intent or intelligence insight into capability are not included in the committee's framework. Threat assessment requires consideration of both an actor's capability and the actor's intent; therefore, to fully analyze the threats posed by synthetic biology, it will be important to



consider areas of concern or vulnerability in the context of information that can shed light on actor intent and capability, such as intelligence information.

Another limitation is that the framework, as currently described, outlines the parameters that should be considered when assessing areas of concern, but does not prescribe a specific methodology for drawing conclusions or a specific methodology for gathering information such as domain expertise. The committee's final report will provide guidance on how the framework can be used to assess areas of concern, consider uncertainty, and prioritize mitigation options, but this demonstration will not encompass all possible methodologies that may be useful.

It is also important to recognize that, although the framework is presented as a table, it is not intended to be used as a rigid "checklist" or algorithm, nor does it include all possible questions or factors that may be relevant. Indeed, the committee recognizes there are inherent risks and limitations to over-institutionalizing efforts to capture concern. Rather, the committee developed the table as a means to help conceptualize the issues that need to be considered, and in particular to encourage those who may use the framework in the future to consider factors related to categories including the use of technology, attributes of actors, and the capability to recognize an attack. Some specific factors within those categories may not apply to a given technology or application, and therefore, it may not be necessary to analyze each row-column intersection (cell) in detail. In addition, it would be inappropriate to consider individual cells in isolation or to assign equal weight to all cells. Rather, it should be expected that the considerations for one factor or technology will often be related to or dependent on other factors or other technologies, and the relative weights afforded to these considerations are likely to vary. It is therefore critical to consider all factors when using the framework to assess concerns, particularly when attempting to compare or rank vulnerabilities.

### **Parameters to Consider**

Although the specific methodologies used in conjunction with the framework may vary, the committee offers some general parameters that can guide the types of information to be considered. In describing the rows and columns within the framework, the committee provides some initial thoughts on questions to help guide assessments of specific technologies or applications, and will in its Phase 2 report provide broader guidance to aid an overarching assessment of vulnerabilities. To help frame and unify this guidance, the committee describes these various parameters in the context of timeframes, uncertainty, scale, and weighting.

#### *Timeframe and Uncertainty*

As the committee works with the framework and develops its findings for the Phase 2 report, the timeframes under consideration will be today, what can be expected five years from now, and what might be expected in more than five years. For each technology area, the committee will endeavor to describe its sense of the technology's viability and trajectory. In addition, the committee will attempt to anticipate how intersections and synergies among different technologies may evolve over time to open up new possibilities. Lastly, the committee will also consider the nature of the changes and how they may impact the answers to questions about each factor; for example, what changes might impact the usability of the technology? In short, to the degree possible, the committee will provide a sense of how the assessment of various row-column intersections may be expected to change over time. By attempting

to assess hypothetical developments that may happen at some point in the future, the committee will operate in a realm of considerable uncertainty. This uncertainty is likely to increase as the committee projects further into the future. While the committee will attempt to capture its degree of certainty, it is well established that there are limitations to experts' ability to accurately describe their degree of confidence. If there are areas that are determined to be particularly critical to informing decision making that also have a high degree of uncertainty, analysis beyond the committee's evaluation may need to be conducted to reduce the level of uncertainty for those factors.

### *Scale and Weighting*

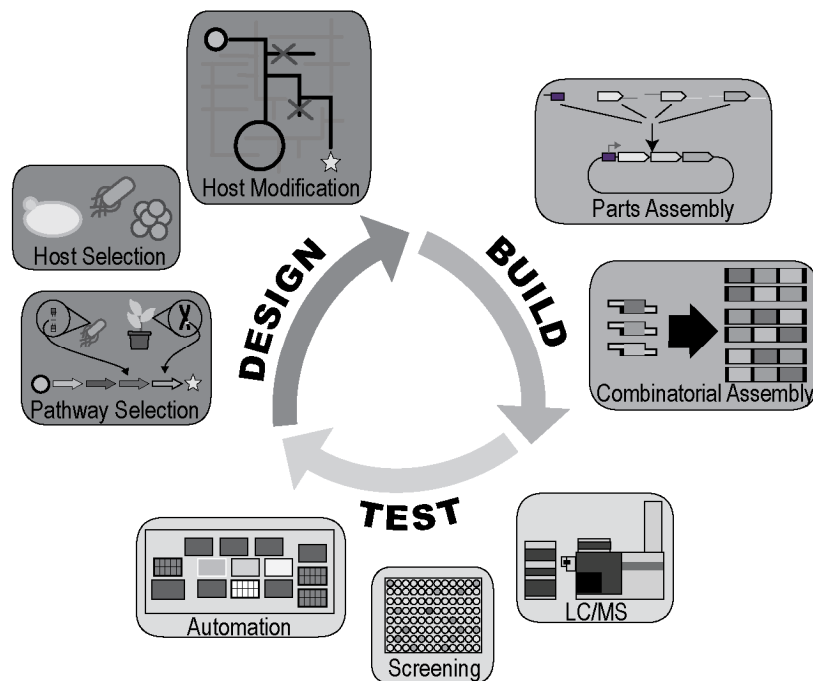
In its second phase of work, the committee plans to use the framework to elucidate where the greatest concerns lie. The committee expects to begin by assigning a level of concern, such as high, medium, or low, to indicate the relative level of concern with regard to a given factor for a given technology area. The committee expects that much of its assessment will rely on primarily qualitative elements, although it is possible that the use of the framework could be expanded in the future to include more quantitative elements than is feasible for this study. Once the relative level of concern has been identified for pertinent row-column intersections, the levels of concern will be compared across the framework as a whole for a broader picture of overall concern in order to help inform the prioritization of agency efforts to address concerns.

The factors identified in the framework, as well as questions listed for each factor, do not all have the same level of importance in determining the overall level of concern, and the importance of any given factor may differ depending on the application. In addition, there may be some interdependencies—"if-then" relationships in which a given technology or factor does not warrant a high level of concern unless another technology or factor is also present. In its Phase 2 report, the committee will use and refine the questions and factors to develop its assessment of concerns; it is expected that considerations for interpreting and appropriately weighting for each factor in the context of drawing overarching conclusions will emerge during this process.

## **ROWS IN THE FRAMEWORK: TECHNOLOGIES AND APPLICATIONS TO ASSESS**

The committee was charged with creating a framework to guide an assessment of the potential security vulnerabilities related to advances in biology and biotechnology, with a particular emphasis on synthetic biology. To reflect the array of biotechnologies that might be considered as part of such an assessment, the committee found it useful to approach synthetic biology technologies and applications from the standpoint of their role in the DBT cycle (see Figure 2). The DBT cycle is fundamental to synthetic biology, and while the technologies used in each of the component phases may evolve over time or be replaced by new technologies, the fundamental concepts of the DBT cycle will stand. Thus, current technologies, as well as anticipated future developments, can be considered in terms of the ways in which they enable the DBT cycle. The committee uses the DBT cycle to frame selected synthetic biology technologies and to evaluate the ways in which those technologies may be applied. While engineering purists may argue that the appropriate cycle is Specify-Design-Build-Test-Learn-Scale or some similar variant, for the purposes of its framework the committee chose to focus on the core elements of the DBT, with additional steps implicitly included in these core elements. For example, Specify is incorporated into Design, Learn is incorporated in the analytical steps of Test, and Scale is

rolled into the overall consideration technologies and applications. Delivery, an important additional step to consider in the context of biodefense, is also an element of Design, for example, when considering cases in which biotechnology may be used to design systems for delivering a bioagent to a target. In its second phase, the committee will also consider how convergence between synthetic biology and advances in other fields, such as materials science and engineering, may affect potential malicious uses of synthetic biology.



**FIGURE 2** Design-Build-Test (DBT) cycle. The committee approached synthetic biology technologies and applications from the standpoint of their role in the DBT cycle, which is fundamental to synthetic biology. NOTE: LC/MS = liquid chromatography–mass spectrometry. SOURCE: Modified from Petzold et al. 2015.

While the DBT framing is useful, its component phases are not strictly separate considerations. There are likely areas in which advances in synthetic biology capabilities relevant to biodefense would arise from synergies or convergence among technologies relevant to different phases. For example, it is important to consider potential synergies between Design technologies and Build technologies, because a malicious actor would need both Design and Build capabilities to carry out an attack. Similarly, synergies may arise if large-scale Test technologies are developed to match the enormous output of certain Build technologies, thus helping those Build technologies reach their full potential. It is also possible, even probable, that some technologies or approaches will have impacts across multiple phases of the DBT cycle; one such example may be directed evolution, where repeated passage in a model host or in cell cultures under stress permits nature to Design, Build, and Test new phenotypes.

In its final report, the committee will present its analysis of the current and emerging synthetic biology technologies that enable each step of the DBT cycle, as well as their anticipated trajectories. In

this report, the committee sets the stage for that analysis by describing areas of biotechnology to consider, along with an indication of the phases with which each area is mostly closely tied (see Figure 2). Numerous advances in the life sciences in the past 10 years have raised concern about possible misuse (JASON 2005, 2007, 2010; IOM/NRC 2006; Blue Ribbon Study Panel on Biodefense 2015; NASEM 2015, 2016; PCAST 2016). While the primary methodology for assessing biosecurity threats in the past has been to rank pathogens of concern, the committee decided not to use such an approach because the tools of synthetic biology can be used in a wide variety of ways and not all potential uses involve pathogens. Similarly, while the acquisition of certain traits has been proposed by the National Science Advisory Board for Biosecurity (NSABB 2015, 2016) as a trigger of concern about gain of function experiments, such a categorization would be too limiting in the context of synthetic biology. Instead, the committee chose to focus on areas in which advances in biotechnology may raise the potential for malicious acts that were less feasible before the age of synthetic biology.

Through its deliberations the committee identified a variety of experimental and computational tools within the DBT paradigm that it considers enabling technologies, in the sense that they have accelerated the pace of discovery and development in synthetic biology. The committee also identified several subcategories of relevant technologies as well as specific potential applications to serve as representative examples. Many of these technologies can be used to pursue multiple ends and could thus raise theoretical concerns related to an array of potential malicious uses. Although these categories and examples are intentionally quite broad and somewhat arbitrary—and do not represent an exhaustive list of all technologies or all possible applications of synthetic biology—it is the committee’s goal that they will provide a useful intellectual foundation that can be adapted to assess new areas of concern as the biotechnology landscape continues to evolve.

The rest of the report will walk through, first, the items for which concern will be assessed, that is, the “rows” in the framework, and then, the factors that the committee is offering as important considerations in determining level of concern, or the “columns” of the framework. For the “rows,” i.e., the technologies and applications being considered, as mentioned earlier these are intended to capture the main items that the committee is aware of at the time of writing, but as the science grows, this list will need to be updated and modified to stay relevant. These rows are also mapped to the DBT phases, as noted in the figure and further discussed in the text.

## **Design**

Technologies and applications most closely aligned with the Design phase of the DBT cycle are those that enable researchers to envision and plan the engineering of biological components. The committee takes a broad view of Design to include both design-enabling technologies and design objectives; as such, this grouping includes both synthetic biology technologies and examples of the types of applications they might enable.

### **Automated Biological Design**

Engineering biological components can be a challenging proposition; organisms are complex, and scientific understanding of biology remains incomplete. Designers must consider the effects of a large array of potential variables, including DNA bases, codons, amino acids, genes and gene segments, regulatory elements, environmental context, empirical and theoretical design rules, and many other

elements. Automated biological design, known in the field as *bio-design automation*, lowers the barrier to designing genetic constructs by automating some decisions and processes that would otherwise require a very high level of expertise or a very long time to carry out. This automation is enabled by tools such as computer algorithms, software environments, and machine learning.

Some automated design tools help researchers specify the desired function of the biological construct or how the parts in the construct will be organized. Other tools help to transform these specifications into collections of realizable DNA constructs; many software tools, for example, help manage and visualize synthetic DNA sequences as they are being designed. Computer software can greatly enhance the designer's ability to predict a design's function and performance, making it more feasible to engineer increasingly complex biological functions and potentially reducing the time and resources required to generate and test designs. Some predictive components of these tools are fairly straightforward, such as the virtual translation of a gene's DNA sequence into the corresponding chain of amino acids. Other functions are more complex, such as the predicted cross interaction of transcription factors in a genetic circuit. There has been significant progress, for example, in the automated compilation of *in vitro* and *in vivo* transcription/translation-dependent genetic circuits starting from high level functional or performance specifications (Brophy and Voigt 2014). Software can also allow designers to create large libraries of combinatorial variants quickly and use machine learning to converge on optimal solutions. This allows for higher levels of design abstraction and the use of standards to exchange information globally between software frameworks.

In addition to aiding biological design, automation tools are used in other phases of the DBT cycle. For example, researchers can use automated assembly tools to plan how to physically create their designed constructs most efficiently, or to send designs created *in silico* directly to remote manufacturing facilities. These designs can be distributed across locations to massively parallelize the construction process. Once a construct is assembled, automated testing tools can be used to verify that it functions as designed. Taken together, a greater predictive capacity, automated assembly, and rapid testing can be expected to facilitate the engineering of increasingly difficult biological functions. Some example applications of automated biological design that are useful to consider in the context of biodefense include design of genes and proteins, and bioprospecting and pathway design.

### *Design of Genes and Proteins*

Automated design programs can create thousands of genetic design variants by combining libraries of genetic “parts” in various ways, an approach known as combinatorial library design. The developers of such programs typically build certain design rules into the algorithm to increase the chances that the designs created will be functional from a biological standpoint. Once the program is in use, the variants it creates can be used to generate new design rules via machine learning. Through this learning process the programs are able to refine subsequent designs; the process also could ultimately remove human designers from the design process, allowing DNA design, assembly, and verification equipment to explore large “genetic design spaces” automatically. The results of combinatorial library design programs can be stored and shared electronically in order for researchers to validate each other's designs, merge multiple designs, or otherwise manipulate the outputs.

Computer-aided design is also being applied to engineer protein structures, which are crucial to many biological processes. Examples of key protein functions being pursued include folding into a desired structure, binding to another protein or to a small molecule, and catalyzing a chemical reaction.

Researchers have already made significant progress toward the predictive design of protein structures and engineering existing peptides and proteins for new functionalities. Automated design tools could facilitate the pursuit of more complex protein engineering, such as designing a new protein or enzyme capable of functioning with a level of specificity similar to that of natural proteins.

### *Bioprospecting and Pathway Design*

Software can also enable designers to search for existing enzymes or biochemical pathways that could be incorporated into genetic designs to produce chemicals of interest. This type of searching is known as *in silico bioprospecting*. Using this approach, researchers systematically screen a large body of DNA sequence data to identify genes or protein domains that encode enzymes capable of performing a desired chemical reaction. After identifying hundreds of candidate genes, researchers produce selected genes synthetically and test their functions *in vitro* or *in vivo*. Additional software tools can be used to engineer more complex biochemical pathways by helping the user visualize those pathways, including their connections to the larger metabolic network of the cell, and estimate how different factors affect the levels of the various compounds produced. In this way, simulation and modeling tools can help to identify where adjustments might be most impactful, such as by increasing the expression of one gene product or by deactivating or downregulating a gene involved in a competing pathway.

### **Metabolic Engineering**

Metabolic engineering involves the manipulation of biochemical pathways within a cell to produce a desired chemical. The desired chemical may be new or one that the cell already makes, and it may be simple (e.g., ethanol) or more complex (e.g., polypeptide or polyketide antibiotics). Based on a detailed understanding of the network of biochemical reactions within the cell, researchers can identify the genes involved in crucial steps in the enzymatic pathways and then adjust them to improve yields. This process is rarely as simple as increasing the expression of all enzymes in the pathway, which can lead to over-consumption of cellular resources and harm the cell's ability to grow and produce effectively. In addition, some intermediate chemical products of the pathway may be toxic to the cell, in which case it can be important to carefully regulate how rapidly such compounds are produced and consumed. Other pathways that compete with production of the final product may also need to be adjusted. Because biochemical pathways are often complex, engineering them frequently involves the use of sophisticated computer software. Metabolic engineering could potentially be used to produce toxins, narcotics, or other products relevant to biodefense. For example, yeast have already been engineered to produce opioids in minute quantities (Thodey et al. 2014). It is also conceivable that these techniques could be used to engineer organisms in the human microbiota to produce compounds that alter human health, perception, or behavior.

### **Phenotype Engineering**

The phenotype of an organism can be affected by multiple genetic components. While there are some phenotypes for which it is possible to identify specific genes or circuits that would need to be added or altered in order to achieve a particular outcome, such as capability for horizontal transfer and transmissibility, in many other cases it is difficult to determine the multiple genetic components that

may impact phenotype. In the past, an organism's phenotypes were manipulated largely by the accumulation of sequential mutations, which in many cases led to local rather than global optimizations of function. More recently, the explosion of sequence information and accompanying systems biology characterizations of multiple organisms have provided a cornucopia of possibilities for engineering phenotypes that involve much more complex networks of genetic components. In parallel, the rise of DNA construction and genome editing technologies could facilitate the construction of multiple variants that involve alterations to multiple genes across an organism. By applying high-throughput screening or selection to these variant libraries, it may be possible to isolate pathogens with dramatically modified phenotypes relevant to their potential weaponization, such as environmental stability, resistance to desiccation, and ability to be mass produced and dispersed.

### **Horizontal Transfer and Transmissibility**

The spread and impacts of a given pathogen are closely tied to its ability to replicate and be transmitted to naïve hosts. Synthetic biology technologies could potentially be applied to make a pathogen's genes more easily transmitted, such as by enabling or enhancing the horizontal transfer of genes (the movement of genes from one organism to another, as opposed to the vertical transfer of genes from parent to offspring). Genes, circuits, or episomes can already be engineered to be horizontally transferred by exploiting commonalities in replication and transformation machinery; for example, the introduction of invasins has been used to alter the host ranges of bacteria (Palumbo and Wang 2006; Wollert et al. 2007). New research aims to combine multiple such techniques to create near-universal horizontal transfer vectors with expanded functionality, which, if successful, could broaden the potential areas of concern (Fischbach and Voigt 2010; Yaung et al. 2014). Combinatorial methods that are available via library synthesis and either high-throughput screening or directed evolution may also potentially be used to alter or expand horizontal transfer and transmissibility. Past research has demonstrated that even low-throughput directed evolution of functions can be used to enhance airborne transmission of H5N1 influenza virus between mammals (Herfst et al. 2012; Imai et al. 2012).

### **Xenobiology**

Xenobiology refers to the study or use of biological components not found naturally on Earth (Schmidt 2010). A simple example is the engineered incorporation of a new amino acid (one not typically found in living cells) into a cell's proteins. Recent research has demonstrated that it is possible to engineer cells to employ a genetic code different from that shared by most life on Earth, or to incorporate non-natural DNA bases (beyond adenine, thymine, cytosine, and guanine) into a cell's DNA (Chen et al. 2016; Feldman et al. 2017). Such approaches could potentially be used to block infection by viruses or prevent undesired horizontal transfer of gene function. Cells with alternative DNA bases, codons, amino acids, or genetic codes may also be able to evade detection based on standard methods such as polymerase chain reaction (PCR), DNA sequencing, or antibody-based assays.

### **Human Modulation**

While past considerations of biodefense concerns have largely been focused on pathogens, synthetic biology raises new possibilities for modifying a person's physiology or environment in ways

that may lead to dysfunction, disease, or increased susceptibility to disease. For example, altering the makeup or functions of the gut microbiome could either enhance a person's health or cause dysfunction. Modulation of the immune system—the body's defense against pathogens—is another hypothetical possibility worthy of consideration, as is epigenetic modification (changes in how cells read genes but not the DNA sequence itself). In short, there is now a large amount of information available about the human form that could potentially inform phenotype modulation in different ways.

## **Build**

Technologies and applications most closely aligned with the Build phase of the DBT cycle are those that are used to physically create actual biological components. Synthetic biology is often pursued in an iterative fashion, blurring the lines among the Design, Build, and Test phases, and some technologies can play a role in multiple phases. Considered here are technological capabilities and advances related to both specified changes and to the construction of libraries for high-throughput screening or directed evolution.

Factors that may impact the level of concern related to Build capabilities include cost, time, and ease of access for DNA construction; the complexity of libraries that can be generated for directed evolution; and the difficulties inherent in rendering the DNA “operable” (that is, the ability to create a synthetic DNA sequence that actually functions within a living system).

### **DNA Construction**

DNA construction refers to technologies that can be used to produce a desired DNA molecule *de novo*. The general and overlapping terms DNA synthesis and DNA assembly are included in this category. Much of modern biotechnology depends on having DNA molecules of defined sequence; synthetic DNA has been used, for example, to advance understanding of the basic workings of the genetic code, to enable modern DNA sequencing, and to develop and enable common use of PCR. In addition, gene editing technologies such as zinc finger nucleases (ZFNs), TAL effector nucleases (TALENs), and CRISPR/Cas9 each depend on some amount of synthetic DNA. Decreasing costs and increased production scales have made it far more feasible to use synthetic DNA for a variety of purposes. Before DNA construction technologies became available, the only way to obtain a particular DNA segment of interest was to find it in an organism. Now, nearly any DNA—whether natural or designed—can be obtained by simply ordering the sequence to be synthesized from one of many commercial suppliers or by making it in a laboratory DNA synthesizer. While DNA is the most common product of DNA construction technologies, these technologies can also be used to create synthetic RNA molecules and chemical modifications to DNA or RNA.

This access is tremendously enabling for the many beneficial uses of biotechnology, but also has ramifications for potential malicious use. For example, DNA construction could conceivably be leveraged to make toxins, enhance a pathogen, re-create a known pathogen, or even create an entirely new pathogen. Generally speaking, ready access to synthetic DNA allows designers to construct, test, and revise their designs more easily. Many DNA synthesis companies have agreed to screen orders in accordance with guidelines from the U.S. Department of Health and Human Services (HHS 2015), although limitations of these guidelines have been described (Carter and Friedman 2015).



Factors that may impact the level of concern related to DNA construction capabilities include cost, time, ease of access, and difficulty of rendering the DNA “operable” (that is, the ability to create a synthetic DNA sequence that actually functions within a living system). The size of a segment of synthetic DNA (a DNA “construct”) is typically described in base pairs for double-stranded DNA and nucleotides for single-stranded DNA. DNA constructs can range from a few nucleotides to several thousand base pairs to entire genomes. Generally speaking, longer DNA constructs are more difficult to produce (or assemble), and using them requires additional laboratory skills compared to shorter constructs. The following examples describe potential uses of DNA construction in ascending order of length and complexity.

#### *Oligonucleotides (Several to Hundreds of Nucleotides)*

In its most basic form, DNA construction produces oligonucleotides (oligos), single strands of user-defined sequence that can range in length from a few nucleotides to a few hundred. Oligos are building blocks used for constructing DNA. Oligos are extremely useful for a wide variety of research tasks that involve manipulating and analyzing DNA, including sequencing and PCR, as well as site-directed mutagenesis and genome-scale gene editing (e.g., using Multiplexed Automated Genome Engineering, or MAGE; Gallagher et al. 2014). While oligos are typically too short to form the types of protein-encoding genes necessary to support more complex biological functions, they can be used to encode regulatory regions (such as promoters or enhancers), certain short polypeptide-based toxins, transfer RNA, and guide RNA molecules such as those employed for gene editing.

#### *Genes (Hundreds to Thousands of Base Pairs)*

Most genes range from a few hundred to a few thousand base pairs in length. Synthetic genes are available commercially as either cloned DNA (in which the product is verified as correct and pure, and typically delivered as part of a general circular plasmid DNA vector) or uncloned linear fragments of DNA (which typically contain some amount of undesired mutations). Potential uses for synthetic genes are at least as diverse as the range of genetic functions found in nature. Genes could be used for a wide variety of malicious purposes, for example, to enhance the pathogenicity of an organism or produce a toxin.

#### *Genetic Systems (Thousands to Hundreds of Thousands of Base Pairs)*

Genetic systems are groups of genes that work together to achieve a more complex function, but fall short of supporting an entire cell. For example, genetic systems could be used to encode a biosynthetic pathway or form engineered genetic circuits that combine operations such as sensing, computing, and actuation. Viral genomes can also be considered as genetic systems, and the genomes for several viruses have already been synthesized and used to produce fully infectious virions (Blight et al. 2000; Cello et al. 2002; Tumpey et al. 2005). Viral genomes can vary from thousands to hundreds of thousands of base pairs in length; large viral genomes (e.g., orthopox viruses) are currently more challenging to synthesize than small ones (e.g., polio).

### *Cellular Genomes (Millions of Base Pairs)*

DNA construction can also be used to assemble the genome for an entire single-celled organism. In 2010, researchers synthesized and assembled the DNA genome of the bacterium *Mycoplasma mycoides* and used that genome to produce a self-replicating cell (Gibson et al. 2010). This was a difficult, time-consuming, and costly process. At about one million base pairs, the synthetic genome was also one of the smallest known in the microbial world. Nevertheless, this feat demonstrated that it is possible to recreate a living, reproducing organism based on its genetic data. In this case, researchers “booted up” their synthetic genome by inserting it into the cell body of a closely related organism, leading to complete replacement of its natural genome with the synthetic one. It remains to be seen how generalizable this approach can be for larger microbial genomes and other types of cells. Other researchers are currently pursuing the construction of bacterial and yeast genomes ranging from 4 to 11 megabase pairs in length; these efforts also use an existing close relative, replacing or “patching” the natural genome with large fragments of the synthetic genome (Richardson et al. 2017). A concern has been raised about the potential for whole genome construction to generate dangerous organisms that otherwise could not be obtained without attracting attention (or might not be obtainable at all), and the committee will consider this and other concerns in its final report.

### **Editing of Genes or Genomes**

A variety of technologies allow the modification of specified bases or genes within a pathogen, vector, or host. Such technologies could potentially be utilized to imbue pathogens with new functions; for example, site-directed mutagenesis capabilities could allow the construction of viral variants with novel properties such as altered immunogenicity or species range. Examples include oligonucleotide-mediated mutagenesis, recombination-mediated genetic engineering (“recombineering”) and related techniques (Murphy and Campellone 2003; Ejsmont et al. 2011), CRISPR/Cas9-based genome editing approaches, and MAGE. Most significantly, newer gene editing platforms such as CRISPR/Cas9 enable the ability to modify a wide range of organisms. Both the ease with which pathogens can be modified and the types of possible phenotypes that could arise from such modifications would be relevant to an assessment of vulnerabilities related to gene or genome editing.

In the past, genome engineering was a painstaking process that required individual genes to be modified serially. Now, however, multiple genes can potentially be modified in parallel, and iteratively. For example, with MAGE, multiple synthetic oligos are created that differ from the existing host genome in at least one base pair. These synthetic oligos are then inserted into a population of cells, where they essentially overwrite the targeted portion of DNA in the cells. The resulting pool of cells can then be screened for desired attributes to identify the oligos associated with these outcomes. This process can create an extremely large set of targeted genetic variants within a population. Because not all sites become modified in each cellular genome, a MAGE experiment employing 20 different oligos (targeting 20 different DNA sites) could produce  $2^{20}$  or approximately 1 million combinations of modified and unmodified sites. MAGE has been used to optimize metabolic pathways, turn off sets of genes, tune gene activity up or down, and engineer a microbial genome with an altered genetic code.

While the biochemical mechanisms MAGE relies on are common throughout both simple and complex organisms, MAGE has primarily been demonstrated in *E. coli* and the work required to adapt MAGE to a new species may prove cumbersome. In contrast, recombineering and CRISPR/Cas9-based

technologies may allow engineering in many new species, providing convenient paths to the further identification of altered phenotypes via either high-throughput screening or directed evolution of organisms with radically new phenotypes and genome-wide sequence changes.

## Library Construction

One of the watershed differences that has been enabled by improvements in DNA construction is the ability to generate large libraries of variants. Such libraries can be sieved for improved phenotypes without knowing precisely what variants will arise. This contrasts with the more deliberate process of gene and genome engineering described in the section titled *Editing of Genes or Genomes*, but overlaps with it because an increased knowledge of how genotype relates to phenotype can guide library design and thereby improve the probability that a given phenotype will be achieved. As an analogy, new DNA construction techniques allow the construction of many more “darts,” and the knowledge inherent in genotype to phenotype relationships provides an increasingly larger “target” to throw those darts at. In particular, the ability to construct degenerate oligonucleotides in a wide variety of ways, including by codon mutagenesis or with nucleotides that are inherently mutagenic, provides a means to construct both large and relatively targeted libraries.

Because DNA can span thousands or even millions of base pairs, designers typically prioritize which parts to vary based on analyses and educated guesses about which changes are most likely to yield the desired results. For example, a designer may use protein structure analysis and visualization software to identify specific parts of a protein that might affect the desired function, such as its enzymatic specificity, build proteins with random variation in those specific parts, and then test how each random variation affects enzymatic specificity.

## Booting of Engineered Constructs

With some exceptions, synthesized DNA (or RNA) does not perform biological functions on its own. The process of inducing raw genetic material to perform biological functions is known as “booting,” a term borrowed from computer technology, where booting refers to the ability to execute functions on digital information by taking it out of storage and putting it into an active state. Booting a synthetic construct is most relevant to the Build and Test phases of the DBT cycle. In the context of biodefense, booting may also be important for a malicious actor’s ability to deliver a bioagent to a target.

Booting in biological systems can take many forms. In the context of viruses, booting may be broadly considered to mean that viral nucleic acids are delivered to cells, where the viral nucleic acids are subsequently able to replicate. A few viruses have been booted by merely delivering their genetic material into host cells, while others require additional genetic components expressed separately in host cells in order to produce infectious viral particles. In the context of bacteria, researchers have successfully booted synthetic bacterial genomes by replacing part or all of the genetic contents of natural or synthesized cells with a partial or full synthetic genome. Booting a fully functioning, self-replicating bacterium is generally significantly more complex than booting a virus.

Perhaps the simplest example of booting engineered constructs is through the use of episomes, pieces of genetic information that can autonomously replicate but cannot for the most part be readily transferred between cells. Plasmids (typically found in prokaryotes) and extrachromosomal linear arrays

of DNA (typically found in eukaryotes) are examples of episomes. Episomes are the most common vector synthetic biologists use to boot engineered constructs, and there are many available techniques to boot episomes. Although episomes in general are not as complex as full viral or bacterial genomes, they can be used to, for example, introduce a viral genome into a cell and then use the host cell's transcription, translation, and replication machinery to boot the virus. It may even be possible to use a similar approach to boot a free-living organism. It is also possible for some episomes to spread through a microbial population and between individuals, albeit in general more slowly than a viral infection would.

## Test

Testing is used to see whether a design or biological product created with synthetic biology tools has the desired properties. Tests are typically performed at many stages of a project; for example, a researcher might use computer models to determine if a design is likely to work, then perform tests to validate that the correct DNA construct has been synthesized, then boot the construct to verify that it is capable of performing the intended biological functions. Testing might involve the use of cell cultures, model organisms in laboratory conditions, organisms in the wild, or even potentially human populations.

Test results can be used to further refine a design, and the DBT cycle begins again. In general, state-of-the-art synthetic biology efforts require a great deal of testing in order to yield organisms with the desired properties, making Test both a crucial step and a substantial bottleneck in the DBT cycle. It is matter of debate whether malicious actors could skip the Test phase and still successfully carry out a biological attack. While a test can be applied to a single variant, in the modern era of synthetic biology the capabilities exist to carry out multiple tests in parallel (high-throughput screening) or to have organisms “test” themselves (directed evolution).

## High-Throughput Screening

Having generated (and transformed or “booted”) large libraries, modern automation provides the means to screen thousands to billions of individual variants of an organism for function or phenotype. High-throughput testing in cell cultures is a type of screening test commonly used in synthetic biology. Such tests can be used to answer more specific questions (e.g., did this precise genomic change yield the desired phenotypic alteration?) or more exploratory questions (e.g., did any of these 100,000 combinatorial variants in one viral protein yield the desired phenotypic alteration?). Technologies for cheaper and faster screening are in high demand across the biological and biomedical communities, in particular for “-omics” approaches that are agnostic to the type of organism being tested, such as DNA sequencing, transcriptomics, metabolomics, and proteomics.

Screening-based tests are performed serially, evaluating different designs or biological products one at a time. Using multiplexing and automation, researchers have developed high-throughput, screening-based tests capable of screening tens to thousands of prototypes. On the other hand, selection-based tests (described in the section titled *Directed Evolution*) are more difficult to design than screening-based tests, but allow much higher throughput.

## Directed Evolution

In nature, the process of evolution selects the best performers from a genetic pool that includes some degree of random variation. Researchers can use a similar process to create prototype biological components representing multiple competing variations and then select among them for the phenotypes that best match the desired outcomes. Prototypes can vary based on smaller changes—different DNA bases, codons, or amino acids, for example—or based on larger-scale differences such as the configuration of multiple genes within a genetic circuit. Like automated biological design, directed evolution is a synthetic biology technique that spans all three phases of the DBT cycle. By building and evolving constructs with random variations, researchers use directed evolution to refine new designs through an iterative approach. However, the primary difference between high-throughput screening and directed evolution is that in directed evolution individual organisms compete for the ability to replicate; for example, genomic variations could be introduced into a modified pathogen, and the entire library selected for the ability to grow in an antibiotic, with only one or a few variants ultimately emerging as successful. Similarly, selection by natural or directed evolution is an especially interesting method by which threats can be “tested,” in that the dictates of evolution (mutation and selection) require both synthesis and selection in parallel. In this regard, directed evolution can be used to evaluate millions of prototype biological components in parallel. These tests can allow a researcher to sidestep the need for predictive design by creating libraries of millions or more variants and then selecting or screening them to find those few that have a desired set of properties. For example, a researcher could randomly alter residues within specific genes or across an entire genome and then select for a desired phenotype, such as growth, tropism, or lysis. Importantly, the selection can be carried out directly in a host organism, thus allowing for the selection of host-related phenotypes, such as infectivity (ability to move from an infected to an uninfected host) or pathogenicity (necrosis within particular tissues). The most promising variants that emerge can be refined further through additional iterations of rational design or selection, following the DBT cycle. Many of the same methods used for library construction and high-throughput screening can also be used for directed evolution, and these different approaches can be combined. For example, a researcher could conduct a high-throughput screen of variants created by a CRISPR/Cas9 library, MAGE, or DNA shuffling (a technique whereby a set of related genes or genomes is broken down into smaller pieces that are re-assembled). The variants selected by the screen could then be selected for growth on a novel substrate, potentially identifying both a gene and an organism whose sequence was not fully included in any of the original precursor genes.

### **COLUMNS IN THE FRAMEWORK: FACTORS FOR ASSESSING CONCERN**

This final section of the report describes the factors that have been identified by the committee as important considerations to include when making the determination of how much concern is associated with a particular technology or application of synthetic biology from the expert perspective. The description of each of the seven factors is followed by subcategories and questions that could be asked by an analyst who was using the framework to assess level of concern. As shown in Box 3, there are two larger categories of factors related to concern—Factors to Assess Capability for Malicious Use and Factors to Assess Capability for Mitigation. Each has several subcomponents, as noted in Box 3 and as described below in each respective section.

### **BOX 3: Columns in the Framework: Factors for Assessing Concern**

#### Factors to Assess Capability for Malicious Use

- Use of Technology
- Use as a Weapon
- Attributes of Actors

#### Factors to Assess Capability for Mitigation

- Deterrence and Prevention Capabilities
- Capability to Recognize an Attack
- Attribution Capabilities
- Consequence Management Capabilities

### **Factors to Assess Capability for Malicious Use**

The ability for a given technology or application to be appropriated for malicious use is influenced by a variety of factors. Some of these abilities are driven by factors related to the capabilities, availability, and use of the technologies involved. Others stem from the ability for the technology or application to be turned into a weapon and cause harm. A third group of factors relates to the attributes of the actors who might potentially be involved in perpetrating an attack.

#### **Use of Technology**

Biotechnology is a fast-moving field. At any point in time, different technologies will be associated with different capabilities, potential applications, costs, and relationships to other technologies. The availability and accessibility of a given technology can also change over time and may be different for different types of users. When analyzing factors related to the use of technology for a given intended application, it is useful to consider questions related to ease of use, rate of development, barriers to use, synergy with other technologies, and cost. Each of these areas is discussed in detail below. Ideally, the questions listed under each subcomponent below should be considered in terms of both the current situation and expected future developments.

#### *Ease of Use*

If a technology is easier to use, it is more likely to be used. This section serves to guide the analysis of technologies in terms of how easy they are to use for a given application. The sections on actor expertise and access to resources are related to this topic, but focus on how the actor's capabilities affect ease of use.

Some technologies are simple, while others require extensive experience; in addition, the use of a given technology may be easier for some applications than for others. Advances in technology have made applications such as creating single nucleotide polymorphisms (SNPs) and adding genes simpler in recent years. Applications that employ combinatorial approaches often involve complex work at large scales—as well as a high degree of unpredictability—thus putting them at the more difficult end of the

spectrum. The availability of detailed information about a specific gene or pathway of interest also affects how easy or hard it is to use available technologies to manipulate that gene or pathway.

Although not all questions will apply in every case, the following questions can help guide an assessment of the ease of use for a given technology and a particular use under consideration:

- How long is the oligo/gene/cassette/genome involved?
- If an entire genome is being created, how easy is it to assemble?
- For an entire genome, how easy is it to “boot”?
- What is the scale and complexity of modification or synthesis involved? For example, is the target a virus, bacteria, fungi, or a larger organism, and how does this affect the ease of use?
- Can the desired construct be ordered commercially, or would regulatory oversight (e.g., Select Agent rules) or construct length make this unlikely?
- Are reagent kits available to make the process easier?
- Are genomic design tools and relevant “parts” databases available to help achieve desired goals?
- How reliable is the available genomic sequence information?
- How reliable is the available genotype-to-phenotype information and how does this affect the ease of use for the intended purpose?
- Is there a recipe or standard operating procedure available for the intended use, and if so, has it been demonstrated to work previously?
- Is specialized equipment required, and if so, is it readily available for purchase or via contract?
- What level of specialized knowledge, hands-on training, and tacit knowledge is required?
- Are suitable test conditions (e.g., cell cultures, model organisms) available?

### *Rate of Development*

The rate of a technology’s development is relevant to assessing the degree of concern that may be warranted at different points in time. Technologies that are developing rapidly are generally of more concern than those that are still predicted by experts to be far off in the future. All technologies follow some form of development curve over time. When considering the rate of development of a technology, it is important to consider the typical development pattern and what that pattern might suggest about the technology’s trajectory, as well as the potential for substantial change over a short period of time (discussed under Barriers to Use). Novel technologies are typically characterized by rapid improvements in accuracy and throughput as their developers try to establish new markets or compete in existing ones. If they survive and gain market acceptance, they enter into a phase of planned growth, with improvements spaced out to allow prior versions to fully amortize their development costs before planned obsolescence. Technologies that have filled a unique market niche may well survive for a long time with only minor improvements in scale or reductions in cost (for example, PCR), while other technologies lose their prominence after being displaced by other innovations (for example, next-generation sequencing is expected to replace pulse-field gel technology for molecular typing of foodborne bacteria; CDC 2016). Technologies that are in common use are likely to be more accessible and therefore more vulnerable to misuse; nonetheless, outdated technologies may still be exploited for harm.

Technologies for de novo synthesis of ever larger DNA constructs and technologies for editing genes and genomes are currently evolving rapidly. For example, the de novo synthesis of all chromosomes from one strain of yeast is expected to be completed soon. The engineering of plants to produce raw or finished chemical products is another area that is maturing rapidly. Assessing the degree to which the rate of development affects the level of concern warranted for a given use of technology should include consideration of both the pace of the technology's evolution and the speed with which it is being adopted. Relevant questions may include

- Are significant improvements to the technology being published on at least an annual basis?
- What aspects are improving? (Examples of aspects to consider include total processing time, cost, laboratory space footprint, level of automation, accuracy, throughput, user interface, and output reporting.)
- What types of uses are driving commercial development and market adoption?
- Is there competition spurring the rate of the technology's development, or does one company have a monopoly?
- Are there multiple different markets for the technology, spurring technological development and innovation, or is it tightly focused on one specific market?
- Is there an open source user community helping to drive the technology forward by sharing new developments?

### *Barriers to Use*

It is also important to consider the presence of significant bottlenecks and barriers, which can lower the likelihood that a technology will be used. For example, key gaps in one aspect of the DBT cycle, such as design knowledge, can significantly limit the potential for malicious use of a given technology and consequently lower the level of concern related to Build capabilities for that technology. Identifying bottlenecks and barriers can also provide insight into potential rapid changes in the rate of development that may be expected in the future, once those barriers or bottlenecks are overcome. This is an especially important consideration in areas of synthetic biology with strong drivers (e.g., beneficial uses attracting significant research) that are pushing the barriers and bottlenecks to be broken. Major technological leaps have the potential to change synthetic biology quickly and open up new possibilities; for example, Gibson Assembly (Gibson et al. 2009) led to a sea change in the capability to compile genetic fragments.

The following questions can be used to assess barriers and the degree to which they may impact the application of a technology for a given malicious purpose:

- Are there critical bottlenecks that, once overcome, will significantly improve ease of use (e.g., CRISPR/Cas9 for gene editing, photolithography for oligo synthesis)?
- What barriers may hinder wider market adoption and penetration of the technology involved, and how might these be overcome?
- Would significant improvements in Build capabilities (e.g., capacity for increased construct length or reduced cost of synthesis) be accompanied by corresponding improvements in capabilities for Design and Testing relevant to the intended application, or would those aspects remain as barriers?



- Are there gaps in fundamental knowledge about pathways and genotype-to-phenotype relationships that may hamper the use of genomic design tools for the intended use?

### *Synergy with Other Technologies*

The capabilities of a given technology can be substantially enhanced by synergies with other technologies. For example, CRISPR/Cas9 can be used alone to make a specific modification to a targeted gene. But when CRISPR/Cas9 is coupled with emerging technologies for single-cell sequencing, it is possible to create random libraries of CRISPR/Cas9 guide RNAs, apply them in parallel to single cells, subject the cells to environmental pressures, and use single-cell next-generation sequencing to identify the “winners”—a far more complex proposition than could be achieved with CRISPR/Cas9 alone.

In the field of computing, Moore’s Law is the business model (Flamm 2004 for National Research Council) that describes the semiconductor technology evolution that has brought ever-greater computing power and data storage at ever-lower costs. At the same time, the evolution of networking technology has converged with computing to make computing ever more ubiquitous, powerful, and inexpensive, thanks in part to a concerted effort to identify and overcome bottlenecks and barriers in both computing and networking. Synthetic biology and sequencing technology may well show a similar convergence in the coming years, in which advances in annotation and predictable sequence-structure-function relationships lead to the ability to reliably design increasingly complex biological systems.

Such developments would have implications for both beneficial and malicious uses of synthetic biology technology. In determining the level of concern warranted for any given technology, it is useful to include consideration of other technologies that may develop in parallel and create opportunities for new types of applications in the future. It is also useful to consider how a breakthrough in one aspect of the DBT cycle might synergize with capabilities in the other aspects; for example, limitations in design knowledge may hinder the full exploitation of certain Build or Test technologies, but if that limitation is overcome, the newly available tools may combine with existing capabilities to enable applications that were not previously achievable.

### *Cost*

Technologies that cost more to acquire or use will affect who is able to use them. The importance of cost as a barrier to use varies depending on the budget of the actor involved: An extremely wealthy lone wolf may have a larger budget for bioterrorism than many poor groups or even some hostile nation-states, for example. The following questions can provide insights on the expected cost of acquiring and using a given technology:

- What are the equipment costs, and how quickly are equipment costs decreasing?
- Are cheaper versions of technology becoming available and are they robust enough to raise concerns?
- Can reagents be acquired from multiple vendors, or is there a secondary market (e.g., eBay) where the equipment can be acquired at a lower cost?
- What are the material or reagent costs?
- What is the shelf life of the required reagents?

- What are the labor costs? Is specialized training required, and if so, what are the costs involved in that training?
- What are the maintenance or service costs and how frequently is maintenance or service needed?
- What facility costs are associated with the technology (e.g., special plumbing, cooling, air flow, filtration, vibration isolation)?
- What is the biosafety risk to the actor, and what costs might be the actor incur to protect the safety of those using the technology?
- What would it cost to conceal the use of the technology from authorities (or other nations)?

## Use as a Weapon

The central question of this study revolves around the degree to which synthetic biology can be used to cause harm—that is, used as a weapon. When analyzing the capability for a given technology to be used as a weapon, it is useful to consider questions related to: production and delivery, the expected scope of casualty for a given use of technology, and the predictability of the intended results. Ideally, these questions should be considered in terms of both the current situation and expected future developments.

### *Production and Delivery*

There are two types of questions to consider with regard to the production and delivery of weapons created with synthetic biology. The first builds upon a large body of existing work related to the classical understanding of the use of pathogens to create weapons of mass destruction. Previous frameworks for understanding threats related to bioweapons outline a series of key steps involved in creating a bioweapon and using it in an attack. These steps include bioagent production, stabilization, testing, and delivery (van Courtland Moon 2006), and might include specific processes like growing large amounts of an agent, milling it into a powder form, making the agent stable enough to be sprayed in a crop duster or withstand other means of mass dispersal, and testing its effectiveness in animal studies. These steps were considered significant barriers to the production of bioweapons in the Cold War era, in effect limiting bioweapons capabilities to a few well-resourced nation-states. In assessing the biodefense concerns posed by biotechnology, it is important to consider: (1) whether synthetic biology could lower the barriers related to bioagent production, stabilization, testing, and delivery, or (2) whether advances in biotechnology areas other than synthetic biology may impact the threats posed by synthetic biology. For example, it may be important to consider how advances in technologies such as bioreactors (a type of biotechnology that is not exclusive to synthetic biology) may change the nature of the production facilities required to produce harmful agents using synthetic biology.

The second type of question is whether synthetic biology makes unnecessary any of these classical steps to weaponization and thus eliminates barriers previously associated with that step. For example, synthetic biology could potentially be used to enhance existing pathogens or create new ones, but it also raises the possibility of types of attacks in which the “weapon” involved is not a pathogen per se, but a genetic construct, toxin, or other entity. Deploying such alternative bioagents might not require the same type of large scale production or purity of pathogens required for some traditional bioweapons. In addition, synthetic biology also could raise concerns about smaller types of attacks that do not require

mass dispersal, which could change the equation with regard to the need for stabilization. All of these factors could potentially reduce or eliminate barriers that previously were thought to hinder the use of bioweapons.

The following types of questions can be used to assess the impact of synthetic biology on the production, stabilization, and delivery of weaponized biological agents for a variety of potential malicious uses. Testing is addressed under Predictability of Result.

- Could synthetic biology (or its use in combination with other biotechnology advances) be used to enhance replication or growth characteristics of an agent in order to support scale-up?
- Could synthetic biology (or its use in combination with other biotechnology advances) help to scale up production of the agent without its losing infectivity or other key features?
- Could synthetic biology be used to make an agent “hardier” in the varied environments it may encounter during storage and delivery (e.g., could it survive the adverse conditions that might be expected in the context of dispersal)?
- Could synthetic biology be used to stabilize the agent or facilitate dispersal and survival?
- How might an agent made with a synthetic biology technology be delivered to those targeted (e.g., mass dispersal, contamination of food or water, a needle stick), and how might this delivery mechanism affect requirements for production, stabilization, or testing?
- Could synthetic biology (or its use in combination with other biotechnology advances) facilitate novel or enhanced forms of delivery?
- Is large scale production of the agent needed to have an impact?
- Could synthetic biology help to reduce the organizational footprint, expertise, or equipment required for production?

### *Scope of Casualty*

The scope of casualty made possible by a given technology or application gives a sense of the scale of the potential threat it poses. The committee identified three dimensions on which to evaluate severity. The first is the classical “degree of disability”—the number of people adversely affected, the duration of the effect, and the level of disability caused, ranging from mild to fatal. The second dimension is the psychological impact on individuals who may or may not be physically affected; this effect can persist after an attack has subsided (Radosavljević and Jakovljević 2007). A third dimension is the degree to which the functioning of the targeted group, organization, or nation is affected by the attack’s medical and psychological dimensions, by the contamination or loss of infrastructure, or by the diversion of staff time and effort toward mitigation or response.

The following questions, developed with consideration of factors described in the World Health Organization’s R&D Blueprint for Action to Prevent Epidemics (WHO 2016), can help to describe the potential scope of casualty when considering the potential impacts of an attack using a given technology or application. Additional factors that are related to the target’s capacity to respond to an attack and limit the scope of casualty are discussed under Consequence Management Capabilities.

- How many individuals could be targeted for harm using this technology (ranging from a single assassination to thousands of people, or more)?

- Is the agent highly transmissible, thus allowing it to spread beyond those affected by the initial attack?
- Would an attack using this technology be expected to be lethal or incapacitating?
- Could an attack using this technology have psychological effects or affect the functioning of the targeted group? For example, could it incite fear, create panic, and/or allow the takeover of a particular region or infrastructure?
- What might the duration of the impact be?
- In what environment(s) might the agent be used?
- Could the agent become established in domestic animals or agricultural livestock (e.g., plague in cats) or wildlife, causing longer-term effects on humans and requiring difficult and costly eradication?

### *Predictability of Result*

Predictability of result describes the degree to which a malicious actor could be confident that the intended result will be achieved when using a given technology to develop a weapon. While some technologies, applications, and types of attack may require extensive testing in order to ensure the intended impact, there may be a lower barrier to success if, for example, the bioagent would only need to be produced one time to have the desired outcome, the attacker has the opportunity to deliver the agent multiple times, or the attacker can create many versions of the agent to maximize the likelihood of success. To assess the predictability of results for the malicious use of synthetic biology, it is useful to consider factors related to testing, fidelity, and phenotype predictability.

*Testing:* A large scale, long-term, and highly resourced bioweapons operation could likely be expected to perform testing prior to deployment to ensure that the scaled-up bioagent behaves as intended and that the delivery or dissemination method is functional. This process would typically involve testing in animal models to ensure illness or lethality, as well as field testing in specific environments to ensure the agent survives well enough to persist and infect targets. In the context of synthetic biology, it is useful to consider the degree to which testing would be necessary for a given use, and how this testing might be carried out.

*Fidelity:* The fidelity of the technology is also an important consideration. For example, do the same procedural steps reproducibly yield the same result, or are the outcomes of a particular technology or method more variable? Newer technologies, or those whose outcomes are more variable, may require an attacker to undertake more research and development before the technology could be reliably weaponized. On the other hand, some well-resourced would-be attackers may be willing to take a chance on using a newer or less reliable technology even if it is not “plug-and-play.”

*Phenotype predictability:* A related question is whether the genotype of a bioagent could be predictably engineered to yield the desired phenotypes. For example, are there known engineering strategies or pre-existing research that outline methods to predictably produce the desired result? Or, can the properties of a bioagent be modeled with computational tools? The ability to predictably design, model, or construct an agent could reduce the need for testing. Agents with predictable genotype-phenotype relationships

may also require fewer resources to deploy, since it may not be necessary to test multiple genotypes to obtain the desired phenotype.

The following questions can help to describe the predictability of result for a given technology or application:

- Does the agent need to be tested extensively to confirm that it is efficacious?
- Is there a relevant animal model for the agent? How predictable is that model for human infection by the same agent?
- What is the fidelity of the technology? How reproducibly can a particular result be obtained?
- Are there known engineering strategies or pre-existing research outlining methods to predictably produce the desired result? Can the properties of a bioagent be modeled with computational tools?
- Is there knowledge regarding the evolutionary stability of an engineered pathogen or pathway? For example, is it likely a synthetic construct will mutate to increase or decrease functionality or activity? Or, can slow-evolving pathogens be generated in order to avoid attenuation?

### **Attributes of Actors**

Any discussion of the concerns related to the potential malicious use of a specific biotechnology needs to include consideration of the person or people who would be involved in perpetrating an attack, here referred to as “actors.” Actors may range from a single individual to a dedicated team to a government body. They may be amateurs, biotechnology experts, engineers, or have some other type of relevant expertise. The complexity, cost, or other barriers to exploiting a technology (see Use of Technology) will have varying levels of importance depending on the capabilities of the actors. For example, while it may be impractical (or would take an extremely long time) for an individual actor to gain the necessary capabilities and knowledge to use a given technology to cause harm, a dedicated team might have the diversity of expertise necessary to enact a plot using the same technology much more quickly.

When analyzing how the attributes of actors affect the level of concern about a given technology or malicious use, it is useful to consider questions related to the expertise an actor would need to possess to effect a given attack, the ability for an actor to access required resources, and the organizational footprint and infrastructure that would be required. This section describes the actor-related questions to consider in assessing the level of concern warranted for a given technology or application. Ideally, these questions would be considered in terms of both the current situation and expected future developments.

#### *Access to Expertise*

Some types or applications of biotechnology require a great deal of expertise in one or more areas, while other uses may require less expertise. The degree to which expertise requirements represent a barrier to malicious use of a technology depends on the expertise possessed (or obtainable) by a malicious actor. It is important to assess the gap between the types of expertise required and the types of expertise actors might be expected to have access to. In some cases, exploiting synthetic biology for harm may require an actor to interact with the conventional research community to acquire goods,

services, or expertise. The following questions, which also relate to ease of use (addressed in the section titled *Ease of Use*, p. 22) and organizational footprint (addressed directly below), are useful in considering how the potential for malicious use of a particular biotechnology might vary depending on the actor's ability to acquire the needed expertise:

- How common and widespread is the technical expertise needed to exploit this technology and could expertise in another, related area suffice?
- Would expertise in more than one area be required to exploit the technology and would the range of technological expertise likely require a group of people to provide the expertise?
- Would the exploitation of this biotechnology require or be enhanced by interaction with the legitimate research community or could the exploitation be performed autonomously?

### *Access to Resources*

The particular resources needed to effect a given malicious use of synthetic biology depend on many factors. Resource requirements can include money, time, laboratory equipment and other infrastructure, reagents and other raw ingredients, personnel and expertise, and other types of resources. Similarly to the considerations relevant to actor expertise (discussed in the sections titled *Attributes of Actors* and *Access to Expertise*), it is useful to assess the gap between the types of resources required for a given malicious use and the types of resources actors might be expected to have access to.

There are multiple ways for an actor to obtain resources. For example, if an actor requires the use of an expensive DNA synthesizer but lacks sufficient funds to purchase a new instrument via conventional channels (or fears an outright purchase would lead to discovery), the actor may consider purchasing a used synthesizer, obtaining legitimate or covert access to equipment at a company or university, coercing an innocent person with legitimate access to perform the work (via bribing, subversion, blackmail, or threats of harm), or resorting to outright theft. A wealthy lone wolf could be better funded than a group sponsored by a poor nation-state. Conversely, a poor but resourceful actor might find ways to access even highly sophisticated technologies, for example, by enrolling in a graduate degree program, getting a job in a biotech company, or taking advantage of relevant service providers or brokers of services. Assessing access to resources is not always a straightforward proposition, but it is nonetheless an important consideration when evaluating vulnerabilities.

### *Organizational Footprint Requirements*

Some malicious uses of synthetic biology might be achievable by an individual working with basic supplies and a rudimentary laboratory, while other types of attacks might require a larger organization, more personnel, or more extensive infrastructure. Considering the organizational footprint that would be required to effect a given type of attack can shed light on the relative importance of other actor attributes, such as access to resources. Organizational footprint also impacts considerations related to mitigation capabilities (discussed in the sections titled *Capability to Recognize an Attack* and *Attribution Capabilities*), such as the ability to identify suspicious activity and prevent an attack, or the ability to attribute an attack to the actor responsible. For example, activities requiring a limited amount of equipment may be able to be pursued by actors with less access to resources and may be conducted in a clandestine laboratory, making detection or attribution more difficult. Malicious uses requiring a large

organizational footprint, on the other hand, might require an actor to have access to more funding or access to legitimate infrastructure (such as by being embedded within a university laboratory), perhaps increasing the likelihood of detection or attribution.

Useful questions to consider include the following:

- What is the organizational footprint (e.g., equipment and other laboratory infrastructure, personnel) needed to utilize the technology?
- Is the infrastructure required to use this technology widespread or rare?
- Could existing organizations or infrastructure be leveraged to use this technology (e.g., dual use of legitimate biotechnology infrastructure) or would the work require a secret facility with a particular set of infrastructure requirements?
- If additional infrastructure would be required for malicious use, would it require an incremental increase in capacity, or major additions?

### **Factors to Assess Capability for Mitigation**

The impact of an attack depends both on the actor's capability to deploy a weapon and the target's capability to prevent, detect, respond to, or withstand the attack. To comprehensively assess vulnerabilities, it is important to consider mitigating factors that may diminish the likelihood that the technology will be effectively used to cause harm, or reduce the damage caused. This section identifies factors that affect the ability to prevent an attack, recognize when an attack has occurred, trace an attack to the responsible actor, and manage the consequences of the attack to care for those affected and limit the spread of the agent.

### **Deterrence and Prevention Capabilities**

Various factors can affect the likelihood that a malicious actor will decide to pursue an attack and then successfully carry it out. One factor that can contribute to deterrence is the availability of countermeasures that limit the amount of harm an attack would cause. For example, the fact that the United States has smallpox vaccine stockpiled—and would thus have a ready countermeasure against an attack using smallpox—is thought to deter malicious actors from perpetrating attacks using smallpox. One factor that can contribute to prevention is the establishment of regulatory and statutory safeguards that limit the ability to access particular pathogens or technologies and use them for harm. For example, by limiting access to certain pathogens, Select Agent rules are intended to help prevent those pathogens from falling into the hands of malicious actors who might seek to use them as a weapon. In addition, activities such as intelligence gathering can contribute to deterrence and prevention by increasing the capacity to identify suspicious activities and intervene before an attack takes place, or to catch and punish an actor after an attack has occurred, as discussed under Capability to Recognize an Attack and Attribution Capabilities.

The following questions can guide an assessment of the degree to which the malicious use of a given technology or application could be deterred or prevented:

- Can the use of the technology be controlled or prevented through regulation or other means?
- Is the technology geographically centralized, or widely distributed?

## Capability to Recognize an Attack

While some actors may intend for their attack to be immediately known (e.g., in order to cause terror), others may seek to affect the target surreptitiously (e.g., in order to debilitate or distract). In either case, it can be expected that most adversaries would seek to conceal their activities while they are planning and preparing to carry out an attack. Intelligence gathering allows authorities to recognize and respond to activities that may indicate an actor is preparing for a biological attack. Some intelligence gathering efforts focus on actors, such as monitoring individuals or groups who have a known intention to carry out an attack and/or those with access to equipment or expertise necessary to develop a bioweapon. Other efforts focus on identifying suspicious activities, such as the procurement of supplies that could be used in a biological attack. Because biotechnology is used for so many beneficial applications, it can be challenging to identify activities, specialized equipment, or other signatures that distinguish suspicious activity from benign activity. Each technology may present different challenges and opportunities in this respect, and the fact that synthetic biology offers multiple technological paths to reach the same end only compounds the challenge.

Once an attack has occurred, recognizing the emergence of an unusual cluster of disease is the first crucial step toward launching an effective response. Being able to differentiate between a natural disease outbreak and purposeful use of a bioagent is vital to preventing subsequent attacks and finding the perpetrators. This knowledge also can inform how medical personnel, public health organizations, and law enforcement or military authorities act to contain the scope of the damage. Public health programs and disease surveillance systems such as those under the purview of the U.S. Centers for Disease Control and Prevention are designed to facilitate the rapid identification and characterization of emerging health threats.

It is important to consider how synthetic biology might affect the ability to identify suspicious activity, recognize when an attack has occurred, and identify who has been targeted. The following questions can guide an assessment of how a given technology or application might change the landscape of options for surveillance and detection:

- To what degree can beneficial and malicious use of this technology be distinguished?
- Are there particular activities or equipment associated with this technology that may indicate when it is being used to prepare for an attack?
- Could the technology be used to engineer an agent that evades typical disease surveillance methodologies (e.g., to cause an unusual constellation of symptoms)?
- Could the technology be used to engineer an agent that evades typical identification and characterization methodologies (e.g., to create an agent that lacks the phenotypes or DNA sequence used for laboratory identification)?
- Would it be possible to assess whether the agent was created synthetically, as opposed to emerging naturally?
- Could the technology enable targeting of particular subpopulations, and if so, could this targeting be detected with available disease surveillance mechanisms?
- Could environmental surveillance (e.g., direct sensing via BioWatch or similar approaches [DHS 2017], animal sentinels, sensing without direct contact [standoff detection]) provide



earlier warning of a bioweapon attack than waiting for ill individuals to present in the public health system?

- Can mining social media in real-time provide indications of when and where an attack or outbreak using this technology might take place, compared to traditional public health surveillance mechanisms?

### **Attribution Capabilities**

The ability to attribute an attack to the actors responsible is crucial because it allows the prosecution and punishment of those involved, and because it helps to prevent those actors from carrying out subsequent attacks. Attacks that use synthetic biology approaches could conceivably be traced using three main categories of evidence: DNA sequencing, genomic properties, and physical properties.

DNA sequencing—the easiest case—could be used to prove that a sample found in a suspect’s lab has genomic material that exactly matches the strain used in an attack. Genomic properties might allow attribution for cases in which the attacker has removed all traces of the engineered material from the production site. For example, if the engineering technique utilized left a “scar” that is seen in the genome of the attack strain, analysis of that scar might indicate the class of vector or other component that was used in the engineering. The physical properties of evidence could also provide clues to trace the source of an attack. For example, biological material recovered from an attack site could be compared with material recovered from a suspect or a laboratory using tools such as mass spectrometry, other proteomic technologies, or visual analysis with electron microscopy or atomic force microscopy.

The following questions can guide an assessment of the attribution opportunities for a given biotechnology:

- How feasible would it be to use DNA sequencing to compare samples of the agent with samples from recovered evidence?
- Would the technique used to construct or modify the agent leave a genomic “scar” that could potentially be used as evidence?
- Would it be possible to identify a design “signature” linking the use of this technology with a given group or laboratory?
- Would the use of this technology be associated with certain physical properties that could be used to compare samples of the agent with samples from recovered evidence?

### **Consequence Management Capabilities**

Protocols and procedures for responding to public health emergencies and bioterrorism attacks exist in both the civilian and military arenas (CDC 2001, 2017). These procedures often involve, for example, epidemiological methods of identifying victims, agents, and modes of transmission, as well as activities such as the development and use of vaccines, drugs, and antitoxins to save lives. Other relevant capabilities include emergency response capacity, availability of supportive health care facilities, and effective procedures for isolation and quarantine. It is important to understand how advances in synthetic biology could change our ability to mitigate the negative impact of an attack.

The following questions can help elucidate whether a given use of synthetic biology could be contained with typical public health measures focused on identifying and controlling the spread of disease:

- Will existing civilian and military public health infrastructure and mitigation approaches to minimize morbidity and mortality be effective against an attack using this technology?
- Are there currently effective medical countermeasures available for an attack using this technology, or would it be possible to quickly develop vaccines, drugs, or antitoxins to mitigate the spread and impact of the agent over the longer term?
- Would the effectiveness of those mitigation approaches rely on knowing how an agent was created?
- Would it be possible to understand the genotype, phenotype, or chemical composition of the agent, to inform how its effect can be mitigated?

## CONCLUSION

Advancements in biotechnology in the 21st century, facilitated by approaches under the rubric of synthetic biology, have the potential to complicate the landscape of possible uses of biological agents to cause harm. In this Phase 1 part of its study, the Committee on Strategies for Identifying and Addressing Biodefense Vulnerabilities Posed by Synthetic Biology assembled a proposed framework that can be used to determine potential concerns posed by these advancements and to inform the identification of vulnerabilities and potential options for mitigation. The framework describes a series of technologies and applications, together with a series of factors for assessing the levels of concern that each of those technologies and applications presents in terms of capabilities for malicious use, as well as factors for assessing capability for mitigation.

In its final report, the committee will use this framework, revising it as needed, as a tool to provide the U.S. Department of Defense with an assessment of the concerns presented by synthetic biology technologies and applications, as well as the possibilities for mitigation, by considering the factors presented here and developing informed answers to questions such as those posed in this interim report.

## REFERENCES

- Blight, K.J., A.A. Kolykhalov, and C.M. Rice. 2000. Efficient initiation of HCV RNA replication in cell culture. *Science* 290(5498):1972-1974.
- Blue Ribbon Study Panel on Biodefense. 2015. A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts. Available at: <https://www.ecohealthalliance.org/wp-content/uploads/2016/03/A-National-Blueprint-for-Biodefense-October-2015.pdf>. Accessed on June 22, 2017.
- Breaker, R. 2017. Presentation at the First Meeting for Committee on Strategies for Identifying and Addressing Biodefense Vulnerabilities Posed by Synthetic Biology, January 26, 2017, Washington, DC.
- Brophy, J.A., and C.A. Voigt. 2014. Principles of genetic circuit design. *Nature Methods* 11(5):508-520.
- Carter, S.R., and R.M. Friedman. 2015. DNA Synthesis and Biosecurity: Lessons Learned and Options for the Future. October 2015. Available at: <http://www.jcvi.org/cms/fileadmin/site/research/projects/dna-synthesis-biosecurity-report/report-complete.pdf>. Accessed on July 5, 2017.
- CDC (U.S. Centers for Disease Control and Prevention). 2001. The Public Health Response to Biological and Chemical Terrorism: Interim Planning Guidance for State Public Health Officials. July 2001. Available at: <https://emergency.cdc.gov/documents/planning/planningguidance.pdf>. Accessed on May 12, 2017.
- CDC. 2016. The Future of PulseNet. Available at: <https://www.cdc.gov/pulsenet/next-generation.html>. Accessed on May 12, 2017.
- CDC. 2017. Preparation and Planning for Bioterrorism Emergencies. Available at: <https://emergency.cdc.gov/bioterrorism/prep.asp>. Accessed on May 12, 2017.
- Cello, J., A.V. Paul, and E. Wimmer. 2002. Chemical synthesis of poliovirus cDNA: Generation of infectious virus in the absence of natural template. *Science* 297(5583):1016-1018.
- Chen, T., N. Hongdilokkul, Z. Liu, D. Thirunavukarasu, and F.E. Romesberg. 2016. The expanding world of DNA and RNA. *Current Opinion in Chemical Biology* 34:80-87.
- Clapper, J.E. 2016. Worldwide Threat Assessment of the U.S. Intelligence Community. Statement for the Record by James R. Clapper, Director of National Intelligence. Senate Armed Service Committee, February 16, 2016. Available at: [https://www.dni.gov/files/documents/SASC\\_Unclassified\\_2016\\_ATA\\_SFR\\_FINAL.pdf](https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf). Accessed on May 19, 2017.
- Cong, L., F.A. Ran, D. Cox, S. Lin, R. Barretto, N. Habib, P.D. Hsu, X. Wu, W. Jiang, L.A. Marraffini, and F. Zhang. 2013. Multiplex genome engineering using CRISPR/Cas systems. *Science* 339(6121):819-823.
- Cummings, C.L., and J. Kuzma. 2017. Societal Risk Evaluation Scheme (SRES): Scenario-based multi-criteria evaluation of synthetic biology applications. *PLOS ONE* 12(1):e0168564.
- DHS (U.S. Department of Homeland Security). The BioWatch Program. Available at: <https://www.dhs.gov/biowatch-program>. Accessed on July 5, 2017.
- DiEuliis, D., and J. Giordano. 2017. Why gene editors like CRISPR/Cas may be a game-changer for neuroweapons. *Health Security* 15(3):296-302.
- Ejsmont, R.K., P. Ahlfeld, A. Pozniakovsky, A.F. Stewart, P. Tomancak, and M. Sarov. 2011. Recombination-mediated genetic engineering of large genomic DNA transgenes. *Methods in Molecular Biology* 772:445-458.
- Elowitz, M.B., and S. Leibler. 2000. A synthetic oscillatory network of transcriptional regulators. *Nature* 403(6767):335-338.
- Esvelt, K.M., A.L. Smidler, F. Catteruccia, and G.M. Church. 2014. Emerging technology: Concerning RNA-guided gene drives for the alternation of wild population. *eLife* 3:e03401.
- Feldman, A.W., V.T. Dien, and F.E. Romesberg. 2017. Chemical stabilization of unnatural nucleotide triphosphates for the in vivo expansion of the genetic alphabet. *Journal of the American Chemical Society* 139(6):2464-2467.

- Fischbach, M., and C.A. Voigt. 2010. Prokaryotic gene clusters: A rich toolbox for synthetic biology. *Biotechnology Journal* 5(12):1277-1296.
- Flamm, K. 2004. Moore's Law and the economics of semiconductor price trends. Pp. 151-170 in *Productivity and Cyclicity in Semiconductors: Trends, Implications, and Questions: Report of a Symposium*. Washington, DC: The National Academies Press. Available at: <https://www.nap.edu/read/11134/chapter/12>. Accessed on May 12, 2017.
- Gallagher, R.R., Z. Li, A.O. Lewis, and F.J. Isaacs. 2014. Rapid editing and evolution of bacterial genomes using libraries of synthetic DNA. *Nature Protocols* 9:2301-2316.
- Gardner, T.S., C.R. Cantor, and J.J. Collins. 2000. Construction of a genetic toggle switch in *Escherichia coli*. *Nature* 403(6767):339-342.
- Gibson, D.G., L. Young, R. Chuang, J.C. Venter, C.A. Hutchison, III, and H.O. Smith. 2009. Enzymatic assembly of DNA molecules up to several hundred kilobases. *Nature Methods* 6:343-345.
- Gibson, D.G., J.I. Glass, C. Lartigue, V.N. Noskov, R.Y. Chuang, M.A. Algire, G.A. Benders, M.G. Montague, L. Ma, M.M. Moodie, C. Merryman, S. Vashee, R. Krishnakumar, N. Assad-Garcia, C. Andrews-Pfannkoch, E.A. Denisova, L. Young, Z.Q. Qi, T.H. Segall-Shapiro, C.H. Calvey, P.P. Parmar, C.A. Hutchison, III, H.O. Smith, and J.C. Venter. 2010. Creation of a bacterial cell controlled by a chemically synthesized genome. *Science* 329(5987):52-56.
- Herfst, S., E.J.A. Schrauwen, M. Linster, S. Chutinimitkul, E. de Wit, V.J. Munster, E.M. Sorrell, T.M. Bestebroer, D.F. Burke, D.J. Smith, G.F. Rimmelzwaan, A.D. Osterhaus, and R.A. Fouchier. 2012. Airborne transmission of influenza A/H5N1 virus between ferrets. *Science* 336(6088):1534-1541.
- HHS (U.S. Department of Health and Human Services). 2013. Framework for Guiding Funding Decisions about Research Proposals with the Potential for Generating Highly Pathogenic Avian Influenza H5N1 Viruses That Are Transmissible Among Mammals by Respiratory Droplets. February 2013. Available at: <https://www.phe.gov/s3/dualuse/Documents/funding-hpai-h5n1.pdf>. Accessed on May 11, 2017.
- HHS. 2015. Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA. Available at: <https://www.phe.gov/Preparedness/legal/guidance/syndna/Pages/default.aspx>. Accessed on May 22, 2017.
- IAC/IAP (InterAcademy Council and The Global Network of Science Academies). 2012. Responsible Conduct in the Global Research Enterprise: A Policy Report. Available at: <http://www.interacademies.net/File.aspx?id=19789>. Accessed on July 5, 2017.
- Imai, M., T. Watanabe, M. Hatta, S.C. Das, M. Ozawa, K. Shinya, G. Zhong, A. Hanson, H. Katsura, S. Watanabe, C. Li, E. Kawakami, S. Yamada, M. Kiso, Y. Suzuki, E.A. Maher, G. Neumann, and Y. Kawaoka. 2012. Experimental adaptation of an influenza H5 HA confers respiratory droplet transmission to a reassortant H5 HA/H1N1 virus in ferrets. *Nature* 486(7403):420-428.
- IOM/NRC (Institute of Medicine and National Research Council). 2006. *Globalization, Biosecurity, and the Future of the Life Sciences*. Washington, DC: The National Academies Press.
- JASON. 2005. Bioengineering. Available at: <https://fas.org/irp/agency/dod/jason>. Accessed on July 5, 2017.
- JASON. 2007. Synthetic Viruses. Available at: <https://fas.org/irp/agency/dod/jason>. Accessed on July 5, 2017.
- JASON. 2010. The \$100 Genome: Implications for DoD. Available at: <https://fas.org/irp/agency/dod/jason/hundred.pdf>. Accessed on May 22, 2017.
- Jefferson, C., F. Lentzos, and C. Marris. 2014. Synthetic biology and biosecurity: Challenging the "myths." *Frontiers in Public Health* 2:Article 115.
- Jinek, M., K. Chylinski, I. Fonfara, M. Hauer, J.A. Doudna, and E. Charpentier. 2012. A programmable dual-RNA-guided DNA endonuclease in adaptive bacterial immunity. *Science* 337(6096):816-821.
- Jinek, M., A. East, A. Cheng, S. Lin, E. Ma, and J. Doudna. 2013. RNA-programmed genome editing in human cells. *eLife* 2:e00471.
- Knight, T. 2003. Idempotent Vector Design for Standard Assembly of Biobricks. MIT Synthetic Biology Working Group Technical Reports. Available at: <https://dspace.mit.edu/bitstream/handle/1721.1/21168/biobricks.pdf>. Accessed on July 14, 2017.

- Mali, P., L.H. Yang, K.M. Esvelt, J. Aach, M. Guell, J.E. DiCarlo, J.E. Norville, and G.M. Church. 2013. RNA-guided human genome engineering via Cas9. *Science* 339(6121):823-826.
- Murphy, K.C., and K.G. Campellone. 2003. Lambda Red-mediated recombinogenic engineering of enterohemorrhagic and enteropathogenic *E. coli*. *BMC Molecular Biology* 4:11.
- NASEM (National Academies of Sciences, Engineering, and Medicine). 2015. International Summit on Human Gene Editing, December 1-3, 2015, Washington DC.
- NASEM. 2016. Gene Drives on the Horizon: Advancing Science, Navigating Uncertainty, and Aligning Research with Public Values. Washington, DC: The National Academies Press.
- Niu, Y.Y., B. Shen, Y.Q. Cui, Y.C. Chen, J.Y. Wang, L. Wang, Y. Kang, X.Y. Zhao, W. Si, W. Li, A.P. Xiang, J.K. Zhou, X.J. Guo, Y. Bi, C.Y. Si, B. Hu, G.Y. Dong, H. Wang, Z.M. Zhou, T.Q. Li, T. Tan, X.Q. Pu, F. Wang, S.H. Ji, Q. Zhou, X.X. Huang, W.Z. Ji, and J.H. Sha. 2014. Generation of gene-modified cynomolgus monkey via Cas9/RNA-mediated gene targeting in one-cell embryos. *Cell* 156(4):836-843.
- NRC (National Research Council). 2004. *Biotechnology Research in an Age of Terrorism*. Washington, DC: The National Academies Press.
- NSABB (National Science Advisory Board for Biosecurity). 2015. Framework for Conducting Risk and Benefit Assessments of Gain-of-Function Research. Available at: [http://osp.od.nih.gov/sites/default/files/resources/NSABB\\_Framework\\_for\\_Risk\\_and\\_Benefit\\_Assessments\\_of\\_GOF\\_Research-APPROVED.pdf](http://osp.od.nih.gov/sites/default/files/resources/NSABB_Framework_for_Risk_and_Benefit_Assessments_of_GOF_Research-APPROVED.pdf). Accessed on May 22, 2017.
- NSABB. 2016. Recommendations for the Evaluation and Oversight of Proposed Gain-of-Function Research, May 24, 2016. Available at: [http://osp.od.nih.gov/sites/default/files/resources/NSABB\\_Final\\_Report\\_Recommendations\\_Evaluation\\_Oversight\\_Proposed\\_Gain\\_of\\_Function\\_Research.pdf](http://osp.od.nih.gov/sites/default/files/resources/NSABB_Final_Report_Recommendations_Evaluation_Oversight_Proposed_Gain_of_Function_Research.pdf). Accessed on May 22, 2017.
- Palumbo, R.N., and C. Wang. 2006. Bacterial invasin: Structure, function, and implication for targeted oral gene delivery. *Current Drug Delivery* 3(1):47-53.
- Parts.igem.org. 2017. Registry of Standard Biological Parts. Available at: [http://parts.igem.org/Main\\_Page](http://parts.igem.org/Main_Page). Accessed on May 19, 2017.
- PCAST (President's Council of Advisors on Science and Technology). 2016. Action Needed to Protect Against Biological Attack. November 2016. Available at: [https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast\\_biodefense\\_letter\\_report\\_final.pdf](https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_biodefense_letter_report_final.pdf). Accessed on May 11, 2017.
- Petzold, C.J., L.J.G. Chan, M. Nhan, and P.D. Adams. 2015. Analytics for metabolic engineering. *Frontiers in Bioengineering and Biotechnology* 3:135.
- Radosavljević, V., and B. Jakovljević. 2007. Bioterrorism—types of epidemics, new epidemiological paradigm and levels of prevention. *Public Health* 121(7):549-557.
- Richardson, S.M., L.A. Mitchell, G. Stracquadanio, K. Yang, J.S. Dymond, J.E. DiCarlo, D. Lee, C.L.V. Huang, S. Chandrasegaran, Y. Cai, J.D. Boeke, and J.S. Bader. 2017. Design of a synthetic yeast genome. *Science* 355(6329):1040-1044.
- Schmidt, M. 2010. Xenobiology: A new form of life as the ultimate biosafety tool. *Bioessays* 32(4):322-331.
- Thodey, K., S. Galanie, and C.D. Smolke. 2014. A microbial biomanufacturing platform for natural and semisynthetic opioids. *Nature Chemical Biology* 10:837-844.
- Tucker, J.B. 2012. *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies*. Cambridge: The MIT Press.
- Tumpey, T.M., C.F. Basler, P.V. Aguilar, H. Zeng, A. Solórzano, D.E. Swayne, N.J. Cox, J.M. Katz, J.K. Taubenberger, P. Palese, and A. Garcia-Sastre. 2005. Characterization of the reconstructed 1918 Spanish influenza pandemic virus. *Science* 310(5745):77-80.
- U.S. Government. 2012. United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern. March 29, 2012. Available at: <https://www.phe.gov/s3/dualuse/Documents/us-policy-durc-032812.pdf>. Accessed on May 11, 2017.

- U.S. Government. 2014. United States Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern. September 24, 2014. Available at: <https://www.phe.gov/s3/dualuse/Documents/durc-policy.pdf>. Accessed on May 11, 2017.
- van Courtland Moon, J.E. 2006. The US biological weapons program. Pp. 9-46 in *Deadly Cultures: Biological Weapons since 1945*, M.L. Wheelis, L. Rózsa, and M.R. Dando, eds. Cambridge, MA: Harvard University Press.
- Vogel, K.M. 2012. *Phantom Menace or Looming Danger? A New Framework for Assessing Bioweapons Threats*. Baltimore, MD: Johns Hopkins University Press.
- Vogel, K.M. 2013. The need for greater multidisciplinary, sociotechnical analysis: The bioweapons case. *Studies in Intelligence* 57(3):1-10.
- Voigt, C.A. 2012. Synthetic biology [editorial]. *ACS Synthetic Biology* 1:1-2.
- White House. 2012. National Bioeconomy Blueprint. Available at: [https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national\\_bioeconomy\\_blueprint\\_april\\_2012.pdf](https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national_bioeconomy_blueprint_april_2012.pdf). Accessed on June 22, 2017.
- WHO (World Health Organization). 2016. An R&D Blueprint for Action to Prevent Epidemics. Available at: [http://www.who.int/blueprint/about/r\\_d\\_blueprint\\_plan\\_of\\_action.pdf?ua=1](http://www.who.int/blueprint/about/r_d_blueprint_plan_of_action.pdf?ua=1). Accessed on June 22, 2017.
- Wollert, T., B. Pasche, M. Rochon, S. Deppenmeier, J. van den Heuvel, A.D. Gruber, D.W. Heinz, A. Lengeling, and W. Schubert. 2007. Extending the host range of *Listeria monocytogenes* by rational protein design. *Cell* 129(5):891-902.
- Yaung, S.J., C.M. Church, and H.H. Wang. 2014. Recent progress in engineering human-associated microbiomes. *Methods in Molecular Biology* 1151:3-25.

## COMMITTEE BIOGRAPHIES

### **Michael Imperiale**, University of Michigan Medical School (*Chair*)

Michael Imperiale, PhD (*Chair*) is the Arthur F. Thurnau Professor and Associate Chair of Microbiology and Immunology at the University of Michigan Medical School. Dr. Imperiale's research focuses on the molecular biology of the small DNA tumor virus BK polyomavirus (BKPyV) and specifically on how the virus traffics through the cell and interacts with the host intrinsic immune functions. Dr. Imperiale is a previous member of the National Science Advisory Board for Biosecurity (NSABB) and has been deeply involved in the policy discussion regarding the potential risks and benefits of gain-of-function research. In 2010, he was elected as a Fellow of the American Academy of Microbiology and a Fellow of the American Association for the Advancement of Science in 2011. He is the founding editor-in-chief of *mSphere* and also serves as an editor for *mBio*. In addition to his laboratory research, Dr. Imperiale is involved in science policy. He serves on the Committee on Science, Technology, and Law at the National Academies of Sciences, Engineering, and Medicine; and on the Planetary Protection Subcommittee at NASA. Dr. Imperiale received his BA, MA, and PhD from Columbia University, all in Biological Sciences.

### **Patrick Boyle**, Ginkgo Bioworks

Patrick Boyle, PhD, is the Head of Design at Ginkgo Bioworks, a Boston-based synthetic biology company that makes and sells engineered organisms. Dr. Boyle's team provides design tools and synthetic biology expertise to Ginkgo's Organism Engineers and is an integral part of Ginkgo's Design, Build, Test, and Ferment strategy for organism engineering. Dr. Boyle has extensive hands-on experience with the day-to-day applications of synthetic biology, as well as with working within the existing regulatory structure surrounding synthetic biology. Dr. Boyle received his PhD in Biological and Biomedical Sciences from Harvard Medical School.

### **Peter A. Carr**, Massachusetts Institute of Technology Lincoln Laboratory

Peter A. Carr, PhD, is a Senior Scientist at the Massachusetts Institute of Technology's Lincoln Laboratory, where he leads the Synthetic Biology research program. His research interests span genome engineering, rapid prototyping of both hardware and wetware, DNA synthesis and error correction, risk evaluation, and biodefense. Dr. Carr is the Director of Judging for the International Genetically Engineered Machine Competition (iGEM) and is deeply knowledgeable about both the practice and potential implications of synthetic biology, with a special focus on the potential impacts on biodefense. Dr. Carr received his bachelor's degree in Biochemistry from Harvard and his PhD in Biochemistry and Molecular Biophysics from Columbia University.

### **Douglas Densmore**, Boston University

Douglas Densmore, PhD, is Associate Professor in the Department of Electrical and Computer Engineering and a Hariri Institute for Computing and Computational Science and Engineering Faculty Fellow, both at Boston University. His research focuses on the development of tools for the

specification, design, and assembly of synthetic biological systems, drawing upon his experience with embedded system-level design and electronic design automation (EDA). He is the director of the Cross-disciplinary Integration of Design Automation Research (CIDAR) group at Boston University, where his team of staff and postdoctoral researchers, undergraduate interns, and graduate students develop computational and experimental tools for synthetic biology. He is the lead investigator for the National Science Foundation Expeditions “Living Computing Project” and a Senior Member of the Institute of Electrical and Electronics Engineers and Association for Computing Machinery. Dr. Densmore received his PhD in Electrical Engineering from the University of California, Berkeley.

**Diane DiEuliis**, National Defense University

Diane DiEuliis, PhD, is a Senior Research Fellow at National Defense University (NDU). Her research areas focus on emerging biological technologies, biodefense, and preparedness for biothreats. Dr. DiEuliis also studies issues related to dual use research; disaster recovery research; and behavioral, cognitive, and social science as it relates to important aspects of deterrence and preparedness. Prior to joining NDU, Dr. DiEuliis was the Deputy Director for Policy in the Office of the Assistant Secretary for Preparedness and Response (ASPR), U.S. Department of Health and Human Services. Dr. DiEuliis also previously served in the Office of Science and Technology Policy (OSTP) at the White House and was a program director at the National Institutes of Health. Dr. DiEuliis has a broad knowledge about the policy implications of emerging technologies, as well as the intricacies that accompany instituting new policies to regulate such emerging technologies. Dr. DiEuliis received her PhD in Biological Sciences from the University of Delaware.

**Andrew Ellington**, The University of Texas at Austin

Andrew Ellington, PhD, is the Fraser Professor of Biochemistry at The University of Texas at Austin. Dr. Ellington’s research focuses on the development and evolution of artificial life, including nucleic acid operating systems that can function both in vitro and in vivo. His lab aims to “[reduce] synthetic biology ... to an engineering discipline rather than a buzzword.” Dr. Ellington was previously a recipient of the Office of Naval Research Young Investigator, Cottrell, and Pew Scholar Awards. He has actively advised numerous government agencies on biodefense and biotechnology issues, including being recently named a National Security Science and Engineering Faculty Fellow. He was also recently named a Fellow of the American Academy of Microbiology and of the American Association for the Advancement of Science. Dr. Ellington has also helped found the aptamer companies Archemix and b3 Biosciences, and has an intimate understanding of both the academic and commercial sides of synthetic biology, as well as the challenges to both.

**Gigi Kwik Gronvall**, Johns Hopkins Center for Health Security

Gigi Kwik Gronvall, PhD, is a Senior Associate at the Johns Hopkins Center for Health Security and Visiting Faculty at the Johns Hopkins Bloomberg School of Public Health. An immunologist by training, Dr. Gronvall’s work addresses how scientists can diminish the threat of biological weapons and how they can contribute to an effective response against a biological weapon or a natural epidemic. Dr. Gronvall is the author of the 2016 book *Synthetic Biology: Safety, Security, and Promise* (Health



Security Press). She is a member of the Threat Reduction Advisory Committee (TRAC), which provides the Secretary of Defense with independent advice and recommendations on reducing the risk to the United States, its military forces, and its allies and partners posed by nuclear, biological, chemical, and conventional threats. Dr. Gronvall had testified before Congress on topics relating to biosafety and biosecurity and is widely regarded as an expert on the role of scientists in health and national security matters. Dr. Gronvall earned her PhD from Johns Hopkins University.

**Charles Haas**, Drexel University

Charles Haas, PhD, is the L.D. Betz Professor of Environmental Engineering and Head of the Department of Civil, Architectural and Environmental Engineering at Drexel University. His broad research interests include the estimation of human health risks from environmental exposures to pathogens and their control using engineering interventions and drinking water treatment. Dr. Haas is broadly knowledgeable in the field of risk assessment, particularly in the context of complex and interdependent systems. Dr. Haas was co-director of the Center for Advancing Microbial Risk Assessment, which was jointly funded by the U.S. Department of Homeland Security and the U.S. Environmental Protection Agency. Dr. Haas has served on a number of National Academies committees, including serving as chair of the Committee to Review Risk Assessment Approaches for the Medical Countermeasures Test and Evaluation Facility at Fort Detrick, Maryland. Dr. Haas received his PhD in Environmental Engineering from the University of Illinois at Urbana-Champaign.

**Joseph Kanabrocki**, The University of Chicago

Joseph Kanabrocki, PhD, is the Associate Vice President for Research Safety and Professor of Microbiology in the Biological Sciences Division of the University of Chicago. Dr. Kanabrocki is tasked with instilling a culture that focuses on the health and well-being of all University personnel engaged in research activities. Dr. Kanabrocki is an expert in biosafety and biosecurity issues, especially practical ones arising from day-to-day laboratory work due to his appointment as Biological Safety Officer and Select Agent Responsible Official for the University of Chicago. Dr. Kanabrocki is a member of the National Institutes of Health Recombinant DNA Advisory Committee (NIH-RAC) and currently a member of the National Science Advisory Board for Biosecurity (NSABB). Dr. Kanabrocki served as Co-Chair of the NSABB Working Group that produced the 2016 report, Recommendations for the Evaluation and Oversight of Proposed Gain-of-Function Research. Dr. Kanabrocki received his PhD in Microbiology from the University of South Dakota School of Medicine.

**Kara Morgan**, Battelle Memorial Institute

Kara Morgan, PhD, is a Research Leader at Battelle Memorial Institute. Her work in public health policy analysis includes developing and evaluating data-driven decision support tools to support effective risk management decision making. She has worked extensively on risk assessment and in particular, on how results from risk assessments can be effectively integrated into decision making processes. Prior to working at Battelle, Dr. Morgan worked at the U.S. Food and Drug Administration (FDA) in several advisory and leadership positions for 10 years. Through her work supporting the National Nanotechnology Initiative during her time at FDA, in 2005 she published one of the first

articles to establish a framework for informing risk analysis about nanoparticles. Her research in expert elicitation, decision analysis, and risk analysis have led to numerous publications developing and applying risk frameworks to decision making about microbial food safety and the pharmaceutical manufacturing quality. She is currently an adjunct professor at the John Glenn College for Public Affairs at The Ohio State University. Dr. Morgan received her PhD in Engineering and Public Policy from Carnegie Mellon University.

**Kristala Jones Prather**, Massachusetts Institute of Technology

Kristala Jones Prather, PhD, is the Arthur D. Little Professor of Chemical Engineering at the Massachusetts Institute of Technology (MIT). Her research interests are centered on the engineering of recombinant microorganisms for the production of small molecules, especially focusing on the design and assembly of biological pathways to target compounds and the incorporation of novel control strategies for regulation of metabolism. Prior to joining MIT's faculty, Dr. Prather worked in Bioprocess Research and Development at Merck Research Laboratories. She has received numerous awards, including a position on the MIT Technology Review's TR35, a list of innovators under the age of 35; the National Science Foundation's Faculty Early Career Development (CAREER) award; and the Biochemical Engineering Journal Young Investigator Award. Prather has been recognized for excellence in teaching at MIT with several awards, including the School of Engineering's Junior Bose Award for Excellence in Teaching, and through appointment as a MacVicar Faculty Fellow, the highest honor given for undergraduate teaching at MIT. Dr. Prather received her PhD from the University of California, Berkeley.

**Thomas Slezak**, Lawrence Livermore National Laboratory

Thomas R. Slezak, MS, is an Associate Program Leader at Lawrence Livermore National Laboratory. Mr. Slezak is a computer scientist, and manages a team of biologists and software engineers to find innovative solutions for diagnosing and characterizing dangerous pathogens. Mr. Slezak's team has developed PCR assays, pan-microbial microarrays (recently commercialized by Affymetrix), and DNA sequence analysis software to support a broad range of pathogen detection and forensic programs in biodefense and human and animal health. Mr. Slezak co-chaired a Blue Ribbon Panel on bioinformatics for the U.S. Centers for Disease Control and Prevention that led to new funding for the Advanced Molecular Detection program, and was a developer of the nationwide BioWatch system. Mr. Slezak has served on three National Academies panels on biodefense topics, as well as on the National Academies' Standing Committee on Biodefense Programs to Advise the Department of Defense. Mr. Slezak received his MS in Computer Science at the University of California, Davis.

**Jill Taylor**, Wadsworth Center

Jill Taylor, PhD, is the Director of the Wadsworth Center and a Faculty Member of the Wadsworth School of Laboratory Sciences. The Wadsworth Center is the only research-intensive public health laboratory in the nation, and Dr. Taylor has served as its Director, Deputy Director, and Interim Director for the past 11 years. Dr. Taylor previously served as the Director of the Wadsworth Center's Clinical Virology Program, which focused on introducing molecular technologies to ensure responsiveness to the

state's changing public health needs, with particular emphasis on influenza virus. As a member of the Board of Scientific Counselors of the U.S. Centers for Disease Control's Office of Infectious Diseases, and a member of the Board of Regents of the National Library of Medicine, she also contributes to policy discussions at the national level. Dr. Taylor is well-versed in developing future research agendas and analysis of new policy proposals and their implications. Dr. Taylor received her PhD from the University of Queensland, Australia.

## **DISCLOSURE OF CONFLICT OF INTEREST**

The conflict-of-interest policy of the National Academies of Sciences, Engineering, and Medicine ([www.nationalacademies.org/coi](http://www.nationalacademies.org/coi)) prohibits the appointment of an individual to a committee like the one that authored this Consensus Study Report if the individual has a conflict of interest that is relevant to the task to be performed. An exception to this prohibition is permitted only if the National Academies determine that the conflict is unavoidable and the conflict is promptly and publicly disclosed.

When the committee that authored this report was established a determination of whether there was a conflict of interest was made for each committee member given the individual's circumstances and the task being undertaken by the committee. A determination that an individual has a conflict of interest is not an assessment of that individual's actual behavior or character or ability to act objectively despite the conflicting interest.

Dr. Patrick Boyle was determined to have a conflict of interest because he is an employee of Ginkgo Bioworks.

The National Academies determined that the experience and expertise of Dr. Boyle was needed for the committee to accomplish the task for which it was established. The National Academies could not find another available individual with the equivalent experience and expertise who did not have a conflict of interest. Therefore, the National Academies concluded that the conflict was unavoidable and publicly disclosed it through the National Academies Current Projects System ([www8.nationalacademies.org/cp](http://www8.nationalacademies.org/cp)).