Sparse Information Mitigation Strategies for Managing Emergent Risk in Synthetic Biology

George Khushf, University of South Carolina
in collaboration with Chris Anderson, UC Berkeley

Our research considers the following questions related to emergent risk, biosafety, and security:

(1) How are questions of risk, safety and security best addressed in an emerging area where there is sparse information for working up risk questions, and where simple allocation of burden of proof along traditional fault lines of precautionary vs risk-based management strategies only leads to polarization and counter-productive posturing? Which aspects of risk, safety, and security can be addressed as technical problems (e.g., design of safe organisms or algorithms for screening orders to sequencing companies) and which aspects are better addressed in terms of institutions and policies and in terms of new forms of governance and/or norms and cultures of responsible innovation? Where are collaborations needed between social impacts/ELSI researchers, scientists and engineers to develop strategies for managing risk, safety, and security associated with synthetic biology? Alternatively, where is research and development best handled in terms of more specialized, disciplinary projects?

(2) How can synthetic biology inform and extend our capacity to monitor and manage risk, assure safety and promote security? Social impacts research is usually oriented toward the ways synthetic biology generates problems of risk, safety, and security. However, the field also provides a host of new tools for conceptualizing and addressing such problems. In what ways might synthetic biology help us better understand and manage risks? Bioinformatics initiatives used to identify commercially viable targets of microbial chemical factories might also enable us to better understand the nature of the risks associated with specific research areas. There are also various technical strategies that can be used to design organisms so they are safe, e.g., to assure containment, establish dependence of organisms on artificial environments, bar code or preserve memory of development that can be used for tracing, or protect with safety mechanisms like kill switches and control circuits. Beyond these technical solutions, synthetic biology offers more general ways of understanding and interfacing with living systems that might inform governance; e.g., evolutionary and combinatorial design strategies commonly used in synthetic biology provide ways of managing systems that remain opaque to users; and new regulatory and control strategies might be generalized to monitor and manage error and failure. Traditional discourse on risk and governance often assumes a capacity to gate, monitor and control technological developments that is unrealistic, and it often requires extensive data that is not available at early stages of research and development. This, in turn, leads to huge discrepancies between the rates of technological development and those of social oversight mechanisms. In what ways do our approaches to risk and governance work with assumptions about how we understand and manage technology that are no longer fit for the practices and products associated with synthetic biology? Are there ways a philosophy of the emerging science and technology can inform approaches to governance that are more agile and better track the current realities of the science?

(3) How do we identify and understand emergent risk? Synthetic biology involves an extension of tools associated with recombinant DNA research and, more generally, molecular biology and biotechnology. The risk space for these antecedent fields has been partially mapped, and there are an extensive range of policies for

managing these risks. When asking about the risks associated with synthetic biology, we are thus not asking about the risks of a technological capacity that is viewed independent of policy. Instead, we are concerned with the differential elevation in risk associated with managing the emerging research as if it were of a conventional sort. The risk associated with an emerging STEM field is the elevated, unmanaged risk that potentially calls for some extension of policy. Mapping this emergent risk is especially difficult because it requires specification of a relevant extension of the emergent field over the conventional field of research together with an appreciation of how this specific difference leads to an elevated residual risk. When does the relevant specific difference involve an unmitigated risk that is above a threshold that calls for an extension of policy to manage that risk? How do we best identify and manage these emergent risks in synthetic biology? Are there strategies that can be used to rapidly work up questions of realistic emergent risks, so we can initiate research that enables us stabilize and extend the policy infrastructure at a rate that roughly tracks the rate of technological development?

(4) What policies and initiatives are relevant when considering emergent risk, and what assumptions about the development, use, and associated practices of technology are implicit in such policies? As noted in (3), emergent risk is a complex function of the difference between emergent and conventional technology and the background policies for managing the conventional risk. To clarify the policy challenge associated with an emergent domain, we thus need to understand the relevant background policy and recognize mismatches between assumptions about technology integral to the policy and the current realities of the technology to be managed by the policy. Similarly, new initiatives to manage risk involve assumptions about technology that may or may not be appropriate; for example, DARPA initiatives assume virulence of a pathogen can be specified at the level of a gene, and thus handled as a modular component that is transported from one organism to another. This assumption also informs strategies for determining biosafety levels of research based on the risk group of the wild type of an organism or that of a gene derived from a pathogen. Related assumptions maintain a focus on select agents when considering bioweapons. Are these assumptions appropriate? Any gap analysis of the policy infrastructure depends on recognizing the messy patchwork of relevant policies and the assumptions about technological types and uses implicit in those policies. How do we clarify the relevant patchwork, identify the problematic assumptions, and advance an understanding of gaps in ways that can constructively inform new, more fitting approaches to governance?

(5) How can we develop forms of risk analysis and management that work with sparse information? In emerging research areas there is often insufficient data for conventional risk analysis. Even in areas where a risk scenario can be specified, many or even all of the steps in the risk pathway may be poorly understood. It may be very costly to obtain data on the probabilities of steps in the risk pathway and obtain reasonable estimates of the harm should the risk scenario occur. Generally, risk analysis is data hungry and expensive, and it can divert resources away from promising lines of research that can have a significant, positive social impact. Strategic decisions must thus be made about where to allocate scarce funds for obtaining risk data and for balancing research on risks against research directed toward promising new applications. Are there ways of understanding and managing risks that are less data hungry, and that can work with the sparse information associated with emerging research in synthetic biology?

We are working on sparse information mitigation strategies that can address these challenges.