

POLICY FORUM

BIOSECURITY

Embrace experimentation in biosecurity governance

We must rethink and test assumptions about relationships between biological research, security, and society

By **Sam Weiss Evans**^{1,2,3*}, **Jacob Beal**⁴, **Kavita Berger**⁵, **Diederik A. Bleijs**⁶, **Alessia Cagnetti**⁷, **Francesca Ceroni**^{8,9}, **Gerald L. Epstein**¹⁰, **Natàlia Garcia-Reyero**¹¹, **David R. Gillum**¹², **Graeme Harkess**¹³, **Nathan J. Hillson**¹⁴, **Petra A. M. Hogervorst**⁶, **Jacob L. Jordan**¹⁵, **Geneviève Lacroix**¹⁶, **Rebecca Moritz**¹⁷, **Seán S. ÓhÉigeartaigh**³, **Megan J. Palmer**¹⁸, **Mark W. J. van Passel**⁶

As biological research and its applications rapidly evolve, new attempts at the governance of biology are emerging, challenging traditional assumptions about how science works and who is responsible for governing. However, these governance approaches often are not evaluated, analyzed, or compared. This hinders the building of a cumulative base of experience and opportunities for learning. Consider “biosecurity governance,” a term with no internationally agreed definition, here defined as the processes that influence behavior to prevent or deter misuse of biological science and technology. Changes in technical, social, and political environments, coupled with the emergence of natural diseases such as COVID-19, are testing existing governance processes. This has led some communities to look beyond existing biosecurity models, policies, and procedures. But without systematic analysis and learning across them, it is hard to know what works. We suggest that activities focused on rethinking biosecurity governance present opportunities to “experiment” with new sets of assumptions about the relationship among biology, security, and society, leading to the development, assessment, and iteration of governance hypotheses.

Traditional international biosecurity efforts have focused largely on risk man-

agement (i.e., addressing accidental and deliberate risks from pathogens and toxins) and dual-use research (i.e., potential malicious exploitation of knowledge, skills, and technology). These efforts assume that we already know what to worry about (lists of known pathogens and toxins) and how to govern it (access control), even if organizations implementing biosecurity recognize the shortcomings and limitations of these assumptions (1).

In the past decade, however, our ability to manipulate living organisms and entire genomes has advanced rapidly through the development of tools such as CRISPR, improved sequencing techniques, and genome synthesis and assembly approaches. This has allowed us to generate microbes, cell types, animals, plants, materials, and tools (e.g., gene drives), all of which have elicited security concerns. Moreover, concern about state and non-state actor weaponization of biology continues (2–4). The following examples show how new approaches to governance, although innovative, are currently sporadic and often ad hoc responses to particular security deficiencies.

After heated debate about two experiments involving the identification of specific mutations in H5N1 avian influenza that enable spread between mammals, the U.S. government developed policies on review and oversight of dual-use research of concern (DURC), requesting federal funding agencies and institutions to review, modify, and/or oversee certain research. Under the assumption that such oversight would be implemented only if minimally invasive, the policies restricted oversight to a subset of work on a subset of known pathogens and experimentally derived traits. Recognizing that these policies still

focus on known pathogens and do not address risks from modification of respiratory pathogens, the United States developed an additional policy focused instead on post-experiment attributes of an organism in 2017. This Potential Pandemic Pathogen Care and Oversight policy was also the first to consider under which conditions such research is ethical. Regular and systematic review of these policies is essential (5) but currently ad hoc.

A decade ago, the U.S. Federal Bureau of Investigation (FBI) Biological Countermeasures Unit decided that countering potential biosecurity events required staying abreast of advances in biology and engaging closely with the life science research community, including universities, companies, and the emerging do-it-yourself (DIY) community labs. This meant building internal scientific expertise and community liaison capacity, both of which were contrary to the public’s image of the FBI and how it operates (6). Moreover, these efforts called on scientists to take responsibility for identifying and addressing potential security concerns.

The American Biological Safety Association (ABSA) International observed that biosafety professionals have been increasingly asked to assess security in addition to safety aspects of research, but do not know how to assess security concerns, and, perhaps more important, how to think about malicious intent and intentional release. ABSA concluded that further training would improve security and promote common biosecurity practices throughout the scientific community through educational opportunities and development of a global biosecurity credential (7).

We do not have perfect knowledge of the ways that biology might be used by malicious actors, or of the best ways to prevent such uses. No a priori reason exists to believe that our original assumptions and hypotheses are optimal. The consequences of getting assumptions wrong, such as a pandemic caused by a laboratory-derived pathogen, are among the strongest arguments for testing a wide range of assumptions in ways that can provide signals of effectiveness prior to catastrophic events.

An experimental approach focuses attention on the need to be systematic and open about analyzing the limitations of existing systems and promoting actions that address or work around them. It also means

¹Program on Science, Technology, and Society, Harvard University, Cambridge, MA, USA. ²Program on Emerging Technology, Massachusetts Institute of Technology, Cambridge, MA, USA. ³Centre for the Study of Existential Risk, University of Cambridge, Cambridge, UK. ⁴Raytheon BBN Technologies, Cambridge, MA, USA. ⁵Gryphon Scientific, Takoma Park, MD, USA. ⁶Netherlands Biosecurity Office, National Institute for Public Health and the Environment, Bilthoven, Netherlands. ⁷Polo d’Innovazione Genomica Genetica e Biologia (PoloGGB), Terni, Italy. ⁸Department of Chemical Engineering, Imperial College London, London, UK. ⁹Imperial College Centre for Synthetic Biology, London, UK. ¹⁰Center for the Study of Weapons of Mass Destruction, National Defense University, Washington, DC, USA. ¹¹Engineer Research and Development Center, U.S. Army, Vicksburg, MS, USA. ¹²Arizona State University, Tempe, AZ, USA. ¹³Pirbright Institute, Pirbright, UK. ¹⁴Joint Genome Institute, U.S. Department of Energy, Berkeley, CA, USA. ¹⁵Nuclear Threat Initiative, Washington, DC, USA. ¹⁶Centre for Biosecurity, Public Health Agency of Canada, Ottawa, Canada. ¹⁷University of Wisconsin, Madison, WI, USA. ¹⁸Center for International Security and Cooperation, Stanford University, Stanford, CA, USA. Email: samuel.evans@harvard.edu

developing better methods to collect data to evaluate the effectiveness of governance, coupled with data sharing across current and future experiments. These meta-level discussions are key for any robust and adaptive governance system (8, 9).

The experimental metaphor does have some limitations. Security governance strategies are designed not to fail catastrophically, and governance has many actors involved in design and implementation. Our use of “experiment” is best understood in terms of deliberate social experiments around the introduction of new technology

for screening teams’ genetic sequences for known pathogens both provided false positives and missed work with potential security implications beyond issues with known pathogens. This lesson led iGEM to transition to a function-based, rather than sequence-based, screening architecture. This new approach is part of iGEM’s commitment to a multi-tiered, iterative security program that seeks to address an adaptive and expanding range of concerns (11).

Thinking about biosecurity governance as an experiment focuses attention on several often underappreciated aspects of gov-

ernance. One of these is the set of assumptions we make in the process of governing, most notably about the structure of science, governing authorities, and their relations to specific security conceptions. These assumptions tend to come in packages. For example, the use of a system of export controls relies on an assumption that science consists of discrete knowledge entities (e.g., published articles or biological specimens), restricting the export of which enhances security. It also relies on seeing threats as likely originating abroad, as opposed to, say, within labs in a country (i.e., an insider threat).

Another example is the assumption that scientists are best placed to govern themselves, which is at the heart of the DURC policies, despite scientists not necessarily having training to identify security risks. This assumption is so firmly rooted in biosecurity governance that questioning it is difficult, and even when it is questioned, gathering evidence to inform governance redesign is challenging (12). However, scientists may have the requisite knowledge to identify measures for assessing and reducing identified risks. In drawing out these assumptions and comparing them across experiments, we can understand more systematically the contexts in which they are likely to hold and where experiments based on different assumptions might be more informative.

A further underappreciated aspect of governance is its iterative and evolving nature. Governance processes and the stakeholder communities continually renew, in response to both changing technological capabilities and changing community and societal conditions. We can take advantage of this to learn from past governance experiments. Currently, learning from governance experiments usually occurs through ad hoc meetings and publications originating from an organic desire to share experiences or from a broader strategy to create space to talk about lived experiences, such as the ABSA Distance Learning Committee.

LEARNING ACROSS EXPERIMENTS

Organizations that fund life science work, oversee it, set or carry out policy regarding it, or engage in it (as researchers, citizens, or other interested parties) may want to experiment with different ways of understanding what counts as a security concern and what should be done about it. In the spirit of learning across experiments, we offer several initial lessons.

In designing a governance experiment, consideration should be given to framing the proposed set of actions in terms of hypotheses, which in turn are based on a set of assumptions about the science, security concerns, and the governing authorities. For example, early presentations given to biotechnology-related groups by the FBI Biological Countermeasures Unit clearly reflected an assumption that biosecurity was different from nuclear or chemical security because pathogens already exist in the environment, and because research into them is conducted by various sectors for numerous beneficial reasons and at different scales throughout the world. The proposed solution was a governing structure that mirrored this dispersed scientific environment, one that was collaborative rather than top-down. Although the FBI gathered baseline data on scientists’ views of law enforcement to inform its outreach activities (13), measuring the effectiveness and outcomes of the activities could have been enhanced if the FBI had considered this proposed solution as a hypothesis and developed a set of metrics to be able to assess, from the beginning, whether



Is re se et eossequo culpa qui doloreh
endion numet vel invelici qui net et
laboribus. Dolupti nihiligniet ut rem
volore corroid que natias inctincta p

and policy, where the focus is on uncertainty, lack of control, and systematic learning (10). This approach places the concept closer to a design-build-test cycle, but with the focus on governing in a complex adaptive space, not on controlling the system.

GOVERNANCE AS AN EXPERIMENT

One current experimental governance approach is the International Genetically Engineered Machine (iGEM) Foundation’s Safety and Security Program. iGEM runs a yearly competition for around 6000 students and community biolab members from more than 40 countries. Each year, iGEM generates a set of hypotheses about how its proposed changes in safety and security governance of the competition might affect teams and lead to better oversight, and reviews cases that tested—or previously were not caught by—its system. Through these reviews, iGEM recognized that processes

ernance. One of these is the set of assumptions we make in the process of governing, most notably about the structure of science, governing authorities, and their relations to specific security conceptions. These assumptions tend to come in packages. For example, the use of a system of export controls relies on an assumption that science consists of discrete knowledge entities (e.g., published articles or biological specimens), restricting the export of which enhances security. It also relies on seeing threats as likely originating abroad, as opposed to, say, within labs in a country (i.e., an insider threat).

Another example is the assumption that scientists are best placed to govern themselves, which is at the heart of the DURC policies, despite scientists not necessarily having training to identify security risks. This assumption is so firmly rooted in biosecurity governance that questioning it is difficult, and even when it is questioned,

such hypotheses held up, and if not, what might need changing. This lesson might involve, for example, structured feedback from community labs about FBI engagement, and routinized sharing across field offices of standard procedures for developing community relationships. Working with social scientists who can help to identify assumptions and develop alternatives that might better align with the goals of governance could be helpful in designing and documenting these experiments in governance (14).

Developing a capacity to quickly identify difficult or unanticipated cases allows for governing processes to adapt and account for them. To the extent possible, sharing case studies—including both failures and “near misses”—in a timely fashion could aid other biosecurity processes greatly. iGEM developed this capacity and quickly put it to work when a 2016 student team claimed to be developing a gene drive. After working closely with the team and experts to understand exactly what was and was not accomplished, iGEM became one of the first places to produce a policy on gene drives. It then wrote up its lessons learned and shared them with the wider biosecurity community.

Learning involves connecting with communities that have tried similar experiments and could build on earlier results. These groups range from networks of community biolabs to international efforts such as the Global Health Security Agenda’s action package on biosafety and biosecurity. Two examples of connecting communities are the leadership programs through the Johns Hopkins Center for Health Security (Emerging Leaders in Biosecurity Initiative) and Stanford University [Synthetic Biology Leadership Excellence Accelerator Program (LEAP)], both of which provide opportunities for policy experts and/or scientists to learn about biosecurity concerns and approaches for addressing those concerns within their networks. Additionally, specific fora such as the Biological and Toxin Weapons Convention Meeting of Experts, or nonstate venues such as the ABSA International Biosecurity Symposium, provide opportunities for stakeholders to engage in biosecurity governance. Developing communication across communities means addressing barriers to communication, such as industrial considerations of competition sensitivity, governmental controls (e.g., export restriction, classification), and differing terminology.

Taking a structured approach to experimental design, periodically reassessing, and cooperating may seem like simple steps to take, but our collective experience suggests that biosecurity efforts over

the past two decades—from promoting self-governance to requiring oversight of pathogen research—have largely not taken these steps. They require thinking beyond the current crisis, testing design choices (e.g., the use of lists), and being willing and able to rethink basic assumptions, such as the idea that both science and security are things that can be governed in isolation from other aspects of society.

An immediate step to expand and revise these lessons is for philanthropies, governments, and others to fund a review of existing biosecurity governance experiments, with the aim of determining how they are being implemented in practice. The findings from such a review could be integrated into policy redesign and could inform networks of biosecurity practitioners. Such a review also would focus on industries and regions of the world that have little to no current biosecurity governance in place. The industrial and commercial development of biology represents a substantial amount of biological research and innovation. Industrial organizations have considerable influence on state governance decisions, and in addition they are trying out biosecurity governance themselves through efforts such as sequence screening in the International Gene Synthesis Consortium, which might benefit from a more experimental design. For many regions of the world without biosecurity governance, getting basic oversight capacity in place is already a major challenge.

The biosecurity community should establish and strengthen shared resources to help groups wishing to establish new governance systems for their communities, such as the Analytical Approach for the Development of a National Biosafety and Biosecurity System, published by the Public Health Agency of Canada. It also should strengthen resources for cooperation and learning across regions of the world, such as the International Network on Biotechnology run by the United Nations Interregional Crime and Justice Research Institute.

Publicly discussing specific instances of biosecurity concern that our governance systems do not cover can itself be an information hazard, but the processes of biosecurity governance may be less of a hazard to discuss. Institutions have many reasons beyond security (such as reputational and intellectual property risks) to not share information, and we encourage the exploration of options to discuss these more sensitive issues. A particularly important challenge is enabling the safe migration of useful lessons between more restricted environments (e.g., classified facilities, industrial operations) and less restricted environ-

ments (e.g., the DIY community). Sharing an evidence base that describes what has and has not worked is a necessary aspect of developing biosecurity governance that simultaneously reduces risk and promotes scientific progress (15).

At present, no capability for systematic learning about the effectiveness and limitations of current biosecurity governance exists. If we can come to understand governance as an experimental space, we will be able to make more than sporadic movement past reactive approaches, and thus protect our economic vitality, academic freedom, and the health and security of our states, people, and environment. ■

REFERENCES AND NOTES

1. D. DiEuliis, V. Rao, E. A. Billings, C. B. Meyer, K. Berger, *Health Secur.* **17**, 83 (2019).
2. C. McLeish, D. Feakes, *Sci. Public Policy* **35**, 5 (2008).
3. L. Stampnitzky, *Disciplining Terror: How Experts Invented “Terrorism”* (Cambridge Univ. Press, 2013).
4. National Security Strategy of the United States (The White House, 2017).
5. Institute of Medicine and National Research Council, *Globalization, Biosecurity, and the Future of the Life Sciences* (National Academies Press, 2006).
6. S. Tocchetti, S. A. Aguiton, *Sci. Technol. Human Values* **40**, 825 (2015).
7. R. L. Moritz, K. M. Berger, B. R. Owen, D. R. Gillum, *Science* **367**, 856 (2020).
8. M. J. Palmer, F. Fukuyama, D. A. Relman, *Science* **350**, 1471 (2015).
9. F. Daviter, in *Learning in Public Policy: Analysis, Modes and Outcomes*, C. A. Dunlop, C. M. Radaelli, P. Trein, Eds. (Palgrave Macmillan, 2018), pp. 145–165.
10. I. van de Poel, D. C. Mehos, L. Asveld, in *New Perspectives on Technology in Society: Experimentation Beyond the Laboratory*, I. van de Poel, L. Asveld, D. C. Mehos, Eds. (Routledge, 2018), pp. 1–15.
11. P. Millett *et al.*, *Appl. Biosaf.* **24**, 64 (2019).
12. B. Rappert, *Front. Public Health* **2**, 74 (2014).
13. N. Hafer *et al.*, *Sci. Progress* (February 2009); www.scienceprogress.org/wp-content/uploads/2009/02/how_scientists_view_law_enforcement.pdf.
14. A. S. Balmer *et al.*, *Sci. Technol. Stud.* **28**, 3 (2015).
15. National Academies of Sciences, Engineering, and Medicine, *Governance of Dual Use Research in the Life Sciences: Advancing Global Consensus on Research Oversight: Proceedings of a Workshop* (National Academies Press, 2018).

ACKNOWLEDGMENTS

The views expressed in the paper are those of the authors and not of any institutions with which they may be affiliated. This document does not contain technology or technical data controlled under either U.S. International Traffic in Arms Regulation or U.S. Export Administration Regulations. We thank participants of the Novel Practices in Biosecurity Governance workshop organized by S.W.E. at the University of Cambridge in July 2019 through the Biosecurity Research Initiative at St. Catharine’s (BioRISC) and the Centre for the Study of Existential Risk (CSER). The workshop was supported with funding from the Hauser-Raspe Workshop Series. S.W.E. was supported by a Schmidt Futures grant and the Templeton World Charity Foundation. J.L.J. and M.J.P. were supported by the Open Philanthropy Project. N.G.-R. was supported by the Future Innovation Fund. D.R.G. is the 2020 president of ABSA. S.W.E. and M.J.P. are on iGEM’s Safety and Security Committee and LEAP. M.W.J.v.P. recently stepped down as Chair of Action Package 3 for the Global Health Security Agenda (GHS). K.B. serves as deputy chair of the GHS Consortium. G.H. sits on the Biosafety Strategic Leadership Group. N.J.H. runs the Joint Genome Institute extended screening for synthetic biology funding distribution.