

# Chapter 9

## Emerging Biotechnology and Information Hazards



**Anna Cornelia Nieuwenweg, Benjamin D. Trump, Katarzyna Klasa, Diederik A. Bleijs, and Kenneth A. Oye**

Biotechnology innovation has never been more accessible to individuals, companies, and (research)organizations. Advances in genetic engineering, declining costs, and improved education have improved access to biotechnologies. Such openness has provided many benefits as biotechnology has been used to address some of the world's most intractable problems. However, increased access to biotechnology tools and knowledge may also pose risks to humans, animals, and the environment (Meyer 2013; Kera 2014; Li et al. 2017; Oye 2012).

Biosecurity policies seek to limit risks of misuse of biotechnology and enabling sciences (Kelle 2009). Material resources such as funding, laboratory access, possession of critical materials, and control over tools are critical components of the broader biosecurity equation but are often not sufficient. Both deliberate malevolent

---

A. C. Nieuwenweg (✉)

Department of CBRN Protection, Netherlands Organization for Applied Scientific Research TNO, The Hague, The Netherlands

Laboratory of Microbiology, Department of Agrotechnology and Food Sciences, Wageningen University and Research, Wageningen, The Netherlands

B. D. Trump

US Army Engineer Research and Development Center, Vicksburg, MI, USA

K. Klasa

University of Michigan School of Public Health, Arbor, MI, USA

D. A. Bleijs

Netherlands Biosecurity Office, National Institute for Public Health and the Environment, Bilthoven, The Netherlands

K. A. Oye

Massachusetts Institute of Technology, Program on Emerging Technologies, Cambridge, MA, USA

and unintentional negligent misapplications of biotechnology require access to information, inspiration, and know-how as well as material resources.

This chapter focuses on how to foster access to critical knowledge for responsible practitioners and developers while limiting information access for malevolent or irresponsible actors. An overview is given of what information hazards mean within the context of the developing field of biotechnology and synthetic biology (which is defined as “apply[ing] standardized engineering techniques to biology and thereby creat[ing] organisms or biological systems with novel or specialized functions (Issues, U.S.P.C.f.t.S.o.B 2010)), and discusses why responsible actors need to appreciate the significance of information hazards.

The first half of this chapter classifies types of information hazards, discusses under which circumstances information may pose hazards, and suggest what can reasonably be done to communicate scientific advances while limiting the potential for information misuse. Biotechnology governance requires a balance of encouragement and education on one hand, and active and passive surveillance of potentially abusable information on the other hand.

The second half of the chapter discusses practical problems associated with acting on these concerns. These tasks are complicated by shifting stakeholder and user bases, as elements of emerging biotechnologies like synthetic biology are increasingly accessible outside of conventional large governmental, university and corporate labs. Likewise, the global accessibility of biotechnology capabilities and education may reduce the ability of national governments to address information hazards from arising, especially in instances where national differences exist regarding norms, values, and ethics of what forms of biotechnology research are permissible.

Though this chapter does not provide a definitive solution to concerns over information hazards, it describes the broad problem and provides directions on how such hazards may be better monitored and addressed in the near future.

## 9.1 What Is an Information Hazard?

Classifying what comprises an information hazard is an inherently subjective exercise. The ability for biotechnology information to be misused is the product of not only the intellectual capacity possessed by the malevolent actor, but also their raw creativity and ability to imagine how a biotechnology or its enabling sciences might be engineered and crafted in a manner that is deliberately harmful. A manner which should at least be somewhat surprising to the broader scientific audience. On the other side of the coin, those who would surveillance and govern information hazards do so while operating under respective political, institutional, and cultural frames and incentives that bias identification and interpretation of such hazards (Lewis et al. 2019).

Though no definition or comprehensive guidance exists for biotechnology’s information hazards, scientists and governments have long been concerned about

how innovative or disruptive advances within various scientific fields might encourage or enable adversaries. As an operating definition, information hazards may be understood as the rate-limiting step that connects a normatively bad actor with the missing inspiration, knowledge, and processes to deploy scientific capabilities for harmful purposes (Bostrom 2011). Within such an understanding, that rate-limiting piece or pieces of information would be difficult or even impossible for the actor or organization to overcome within a set timeframe through independent research and development.

What makes the governance of information hazards so difficult is the varying forms that information hazards may take. The most intuitive example includes instances where a malevolent actor lacks some core competency or critical piece of intelligence to develop and deliver a hazardous material. Likewise, however, other cases may include malevolent actors which do have advanced basic and research capabilities to foster such threats, yet lack the inspiration, motivation, or direction to act upon that knowledge. Recent decades have largely focused upon the former example, although the latter is equally disconcerting for biotechnology given increasing levels of access to potentially dual-use scientific information to actors with limited institutional oversight from longstanding authorities.

Perhaps the most well-known exercise of governance of information hazards includes government secrecy programs, where certain scientific research was restricted in knowledge and access to approved parties only. Historically, for centuries governments have kept tight control over scientific projects that might yield a strategic advantage in military situations. They were eager to use such scientific advantages as a force multiplier against their enemies yet concerned about losing such strategic advantage should knowledge of how the technology is developed or deployed be made available to other nations. Within the twentieth century, various governments have developed and maintain information classification systems, whereby sensitive intelligence with the potential to foster harm to national security is collected and protected in a range of secure information systems.

The Manhattan Project provides a clear example of information hazards. The US nuclear weapons program in World War II rested on advances in basic and applied sciences. The very existence of the program and core discoveries and scientific breakthroughs were held closely, with no public dissemination. Personnel with access to files were carefully vetted to prevent information spillage to adversaries. Information hazards then and now include the capacity to inspire or educate potential developers. Yet important differences exist (Aldrich et al. 2008).

Today, concerns focus on how easily information might be transmitted from secure research facilities and information storage systems to foreign governments and organizations. Until recently, the primary mode of transfer for such information hazards was either through theft or copying of physical paper documents, or the acquisition of certain scientific personnel with knowledge of the specific information by means of bribery, kidnapping, or similar measures.

With the increasing maturity of high-speed Internet, prior barriers to the transfer of information hazards have been significantly degraded. The robust government classification systems continue to operate around the world, information hazard

spillage is an increasing concern. Prior information hazards, such as the Anarchist's Cookbook, could spread globally through print media, yet lack the immediacy and far superior range that Internet dissemination has been demonstrated to have in virtually all countries.

Like many other emerging sciences like chemistry, nuclear physics, engineering, and computer science, biotechnology is rife with information hazards. Popular literature is riddled with examples of how a malevolent actor might manipulate a pathogen or deployed biological weapon whose consequences are sweeping and often irreversible. The difficulty of identifying and governing information hazards and biotechnology is that the core technical and scientific knowledge that might enable the creation of a weapon could also yield untold benefits to broader society (Lewis et al. 2019; Casadevall et al. 2014). This governance challenge is one of managing dual-use information, where the dissemination access to such information requires an implicit trade-off between the benefits of technological innovation to medicine, industry, and various other fields, against the potential that it might be deliberately or negligently misused. This challenge is not a new one - the example of knives might be overly simplistic yet apt, they can cut food and be useful tools in a workplace, yet also be utilized for the explicit purpose of harm to humans or animals.

Biotechnology information hazards can appear in many forms, and will undoubtedly shift as technologies continue to progress in their sophistication and accessibility. They might include the genetic sequence of a particularly high-risk pathogen, or instructions regarding how to assemble, use, and customize equipment that facilitates more precise and targeted genetic modification. Likewise, it may include the inspiration for deploying biotechnology assets and capabilities in previously unconsidered vectors or receptors of risk, the outcomes of which may have benefits and risks simultaneously.

## 9.2 When Do Information Hazards Matter?

If information hazards are a recurring fixture of human scientific progress, why is it that they matter so much now, and why specifically to biotechnology? As noted above, the Internet is an important consideration here, yet the advancements of biotechnology in and of itself are influencing information hazards trade-offs in a manner where the threat of a malevolent or grossly negligent actor is far more likely in the coming years than in decades past. With the continued refinement of biotechnologies like synthetic biology, information hazards have become increasingly central to biosecurity for two reasons.

First, the ability to synthesize DNA has undercut the effectiveness of physical controls on materials to keep pathogens out of the hands of malevolent and negligent actors (Oye 2012). Limits on access to pathogens on the select agents list and controls on the transportation of pathogens under the Australia Group guidelines are still of critical importance (Rappert and McLeish 2012; Kadlec et al. 1997; Danzig

and Berkowsky 1997). But the ability to synthesize pathogens from information on sequences provides a pathway around physical controls. This aspect of information hazards will become more acute as gain-of-function research produces information on how to edit or modify pathogenic sequences to increase infectivity and virulence (Noyce and Evans 2018).

Second, within the past decade, a keystone achievement of genetic engineering and synthetic biology centers around the de-skilling of certain portions of biotechnology research, enabling those with far less training and experience than in previous decades to conduct advanced biotechnology exercises (Mukunda et al. 2009). Historically, a significant limitation of information hazard transference to malevolent parties included the reliance upon (a) professionals with the graduate education in a biotechnology-relevant field, and (b) considerable financial, technical, and overhead resources to execute scientific development.

To be sure, much of the advanced research that comprises synthetic biology still does require significant training, and certain exercises and tools are still inaccessible to many individuals and organizations around the world. However, this roadblock has diminished over time as the financial costs of conducting biotechnology research in certain sectors has decreased, and experimental control and efficacy has increased for those with a moderate degree of interest in trading. Likewise, as broader biotechnology becomes more globalized through improved training, sharing of information through popular media and academic publications, and global exchanges of scientific ideas and commercial products, biotechnology research is being pursued in locations around the globe, including laboratories, institutions, companies, and schools that do not have a long-standing track record of compliance and oversight with respected institutional authorities (Millett et al. 2019).

As the benefit of skilled premiums is somewhat lessened through cheaper and more accessible biotechnology research strategies, many more individuals with various backgrounds, motivations, and interests in the execution of biotechnology research are gaining entry to the field. One popular field leading the way gene editing, the scientific potential of which is influenced by the decreasing cost of genome sequencing and synthesis on one hand, as well as simplified, relatively inexpensive, and increasingly precise tools and machines to facilitate gene editing experimentation. For the most part, this development should be celebrated, for it enables the development of biotechnology in more cost-constrained settings in a manner that improves educational opportunities while also furthering scientific curiosity and development. However, this leaves government decision-makers and other key stakeholders in a precarious balancing act.

### 9.3 How Might Information Hazards Be Governed?

A critical challenge for the governance of information hazards includes the trade-off of: how can we best educate and train those who might assist with information hazards management without surrendering excessive knowledge that may inspire a malevolent actor in the first place?

There are few straightforward answers to inform biotechnology governments for this problem. Most likely, information hazards governance will have to be an anticipatory as well as an adaptive process, whereby potential information hazards are continuously evaluated accounting for the potential benefits if such information is further democratized against the potential threat that such information may be easily used for nefarious purposes. Examples include research into unknown human pathogens, as well as the deployment of engineered organisms to manipulate environmental conditions for a predetermined purpose (e.g., ‘biomining’). In such cases, those with oversight roles and responsibilities will be required to consider, at a minimum, whether research in these fields has a discernible positive outcome that is a net improvement over conventional scientific capabilities or commercial products. Experiments requiring material from the Select Agent and Toxin List will likely always require some degree of oversight and information classification, including restrictions on how discoveries from such research are communicated.

For other experiments that do not include known agents or toxins of concern, the interpretation of what is and what is not an information hazard becomes far murkier. There are few ready-made answers, and the concern that research with information hazard potential may arise outside of government, university, incorporate labs thorough and established oversight protocols and Institutional Review Boards (IRBs) is increasing. The best advice for information hazards governance at-present therefore includes greater emphasis upon soft law mechanisms for oversight as well as increasing collaboration between top-down and bottom-up actors in the biotechnology space. In decades past, biotechnology governance has been broadly informed by operating principles and codes of conduct that, though they have little legal enforcement, have considerable influence on the norms and expectations of various actors from differing institutions. One renowned example includes the Asilomar Conference on Recombinant DNA, which was initially formed in 1975 to discuss ethical and risk-based hazards stemming from emerging biotechnology research of the day. Comprised of dozens of industry professionals from a variety of institutions, the Asilomar Conference helped to frame and anticipate future safety and ethics concerns that might arise as the field continues to develop, as well as to provide the basis for improved codes of conduct, as well as future regulatory codes and rules inspired by the precautionary principle. Further, efforts such as Asilomar help promote awareness and trust by the broader public that more effective biotechnology governance is being discussed and constructed, potentially making consumers more amenable to such products as they reach the market.

Several illustrative cases exist, were publication sparked debate among policymakers and scientists. Perhaps the most famous case, is the H5N1 gain of function

experiments that focused on whether and which mutations would result in a virus capable of being transmitted to mammals (Herfst et al. 2012; Imai et al. 2012). Knowledge about the specific mutations leading to certain gain of functions can be easily misused by malevolent actors. The controversy of H5N1 gain of function experiments lead to a self-imposed moratorium by scientists (Fouchier et al. 2012) after details from two manuscripts on H5N1 were omitted on behalf of the National Science Advisory Board for Biosecurity (Casadevall and Shenk 2012). Additionally, the Dutch Government required the authors of the paper to file for an export license to prevent export of dangerous information outside of Europe (Enserink 2015).

By way of contrast, the International Genetically Engineered Machine (iGEM) competition provides a case of early and ongoing engagement with biosafety and biosecurity risks. This global synthetic biology competition engages with thousands of high school students, undergraduates, graduate students, entrepreneurs, and community laboratories annually. Student teams work closely with coaches and contest judges to ensure compliance with all legal requirements, as well as to monitor potentially hazardous or dual-use team projects. Judges and support staff are drawn from a number of institutions, including government, but with emphasis placed upon more bottom-up governance of the competition. iGEM serves as one successful example of how improved educational opportunities alongside respected and trusted authorities can both improve global education of synthetic biology and broader biotechnology research, yet simultaneously maintain oversight and awareness of interest and activities occurring outside of large government institutions, corporate offices, or academic laboratories (McNamara et al. 2014; Millett et al. 2019).

Other critical components of bottom-up information hazard governance includes responsibility and decision-making in the publication process. Globally, the publishing industry in virtually all fields has exploded in recent decades, with biotechnology as no exception. Like the democratization and globalization of biotechnology, this should be celebrated, but also reviewed for potential opportunities to improve overall governance. For emerging biotechnologies, this may include more rigorous training for editors and associate editors regarding how to identify potential information hazards, as well as to select qualified and responsible article reviewers to make an appropriate determination. This challenges wrought with the difficult quagmire, whereby journal editors and reviewers must be given greater instruction about which information hazards to look out for, as well as possible examples of them, yet simultaneously not be given enough information that would comprise an information hazard in and of itself. Academic publication remains one of the easiest ways to transfer knowledge of scientific breakthroughs globally, with higher impact in prestigious journals having tens to even many hundreds of thousands of readers on a weekly to monthly basis. Identifying and training operators of those journals that have a reasonable potential to have paper submitted to their journal that may contain information hazard is an urgent need, particularly in standardizing how potential or confirmed information hazards material should be treated within the publication process as well as without. Such measures will likely only be a low fence to prevent spillage of information hazards, yet journal editors and reviewers



will likely be one of the first and possibly only lines of defense that many countries have with respect to information hazards governance on a day-to-day basis.

A long-standing challenge of biotechnology governance related to information hazards includes the construction of all offensive biotechnology capabilities (e.g., biological weapons). The 1975 Biological Weapons Convention prohibits the development, production, and stockpiling of biological and toxin weapons, including all microbial or other biological agents and toxins as well as their means of delivery. The critical distinction includes a focus on offense of use, for which all experimentation is to be prohibited. However, the Biological Weapons Convention makes exceptions for medical and defensive purposes in small quantities, leaving a window open for certain controlled experimentation to continue, provided that any quantities of biological material used and stored are justified in their permitted purpose. The BWC's restrictions have been generally successful in the decades that followed its passage, despite infamous examples of biological weapons programs continuing even after the host government signed the treaty. The important distinction for information hazards is that some research on certain biological material with a medical or defensive purpose will likely inherently have some offense of capability within the hands of a malevolent actor, making it critical to consider the level of oversight and information classification that should be applied to such cases. In addition, special consideration should be given to international research programs that include participation from one or more countries that are known BWC violators or are parties of concern, given the potential for any research or knowledge gained from medical or defensive experimentation to be utilized for other unpermitted purposes.

These and various other exercises that must come to comprise information hazards governance must take on anticipatory and adaptive governing capabilities (Esvelt 2018). Anticipatory, due to the evolutionary nature of biotechnology research, where breakthroughs enable significant departures from one school of thought and into another, thereby fostering new opportunities for information hazards and biosecurity threats to arise. Adaptive, due to the fact that risk assessors and various other decision-makers in the biotechnology governance process iteratively adjust their perception of a given biological threat over time, whereby new information is gained and best practices are adjusted to accommodate for new practices on how the deployment of genetically altered material onto humans, animals, and the environment may generate unacceptable risk. Both anticipatory and adaptive governing procedures for biotechnology within a given country must include a multi-stakeholder approach to inform best governing practices in the years ahead.

## 9.4 Information Hazards: Where Do We Go from Here?

To date, thankfully, there has been no major disaster pertaining to emerging biotechnologies on the scale of Chernobyl or Fukushima Daiichi. This is due in no small part to many well-trained scientists, practitioners, and policymakers that have been



actively engaged with international biosecurity governance for several decades. However, as the pace of biotechnology innovation accelerates, existing hard law procedures and practices will be necessary but potentially not sufficient to fully capture shifting development capabilities and incentives in the development and commodification of biotechnology research and products.

This chapter's intent was not to solve the question of the information hazard governance dilemma, but instead to highlight why it is particularly important for emerging biotechnologies like synthetic biology. Each year, more actors become interested and involved with emerging biotechnology research, including differing cultures and governments differing perspectives on ethical, legal, moral, and risk-informed best practices for biotechnology moving forward. Navigating these intricate differences will be a considerable challenge, both for biotechnology intended for environmental deployment, as well as within human subjects' research. One conclusion that can be drawn now is that top-down hard law mechanisms alone will be generally insufficient to bridge the gap between these differing national incentives and research practices, as well as to adequately monitor the rapid growth of bottom-up biotechnology research.

Over the next several years, information hazards governance will likely become an increasing discussion point within broader biotechnology policy as well as expected practice within the lab. Continued innovation in the biotechnology space will see decreasing cost underpinning such research, such as with the dramatically decreased time and financial resources required to sequence and synthesize a genome, allowing many more actors to take advantage of such scientific breakthroughs. Future conversations about improving biotechnology governance must include improved education and awareness about such concerns in a manner that does not dis-incentivize responsible research, as well as testing and implementing anticipatory and adaptive governance bodies and operating practices that can keep pace with the accelerating rate of biotechnology innovation (Esvelt 2018; Trump et al. 2020).

## References

- Aldrich S, Newcomb J, Carlson R (2008) Scenarios for the future of synthetic biology. *Ind Biotechnol* 4(1):39–49
- Bostrom N (2011) Information hazards: a typology of potential harms from knowledge. *Rev Contemporary Philos* 10:44–79
- Casadevall A, Shenk T (2012) The H5N1 manuscript redaction controversy. *Am Soc Microbiol* 3(1):e00022-12
- Casadevall A, Enquist L, Imperiale MJ, Keim P, Osterholm MT, Relman DA (2014) Redaction of sensitive data in the publication of dual use research of concern. *Am Soc Microbiol* 5(1): e00991-13
- Danzig R, Berkowsky PB (1997) Why should we be concerned about biological warfare? *JAMA* 278(5):431–432
- Eserink M (2015) Dutch appeals court dodges decision on hotly debated H5N1 papers. *Science* 16:89–97

- Esvelt KM (2018) Inoculating science against potential pandemics and information hazards. *PLoS Pathog* 14(10):e1007286
- Fouchier RA et al (2012) Pause on avian flu transmission research. *Science* 335(6067):400–401
- Herfst S et al (2012) Airborne transmission of influenza A/H5N1 virus between ferrets. *Science* 336(6088):1534–1541
- Imai M et al (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
- Issues, U.S.P.C.f.t.S.o.B (2010) New directions: the ethics of synthetic biology and emerging technologies. Presidential Commission for the Study of Bioethical Issues
- Kadlec RP, Zelicoff AP, Vrtis AM (1997) Biological weapons control: prospects and implications for the future. *JAMA* 278(5):351–356
- Kelle A (2009) Synthetic biology and biosecurity: from low levels of awareness to a comprehensive strategy. *EMBO Rep* 10(S1):S23–S27
- Kera D (2014) Innovation regimes based on collaborative and global tinkering: synthetic biology and nanotechnology in the hackerspaces. *Technol Soc* 37:28–37
- Lewis G et al (2019) Information hazards in biotechnology. *Risk Anal* 39(5):975–981
- Li P-E et al (2017) Enabling the democratization of the genomics revolution with a fully integrated web-based bioinformatics platform. *Nucleic Acids Res* 45(1):67–80
- McNamara J, Lightfoot SB-Y, Drinkwater K, Appleton E, Oye K (2014, December) Designing safety policies to meet evolving needs: iGEM as a testbed for proactive and adaptive risk management. *ACS Synth Biol*
- Meyer M (2013) Domesticating and democratizing science: a geography of do-it-yourself biology. *J Mater Cult* 18(2):117–134
- Millett P et al (2019) Developing a comprehensive, adaptive, and international biosafety and biosecurity program for advanced biotechnology: the iGEM experience. *Appl Biosaf* 24(2):64–71
- Mukunda G, Oye KA, Mohr S (2009) What rough beast: synthetic biology and the future of biosecurity. *Politics Life Sci* 28(2):2–26
- Noyce RS, Evans DH (2018) Synthetic horsepox viruses and the continuing debate about dual use research. *PLoS Pathog* 14(10):e1007025
- Oye KA (2012) Proactive and adaptive governance of emerging risks: the case of DNA synthesis and synthetic biology. International Risk Governance Council, Geneva
- Rappert B, McLeish C (2012) A web of prevention: biological weapons, life sciences and the governance of research. Routledge
- Trump BD, Galaitsi SE, Appleton E, Bleijs DA, Florin MV, Gollihar JD, Hamilton RA, Kuiken T, Lentzos F, Mampuy R, Merad M (2020) Building biosecurity for synthetic biology. *Mol Syst Biol* 16(7):e9723

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

