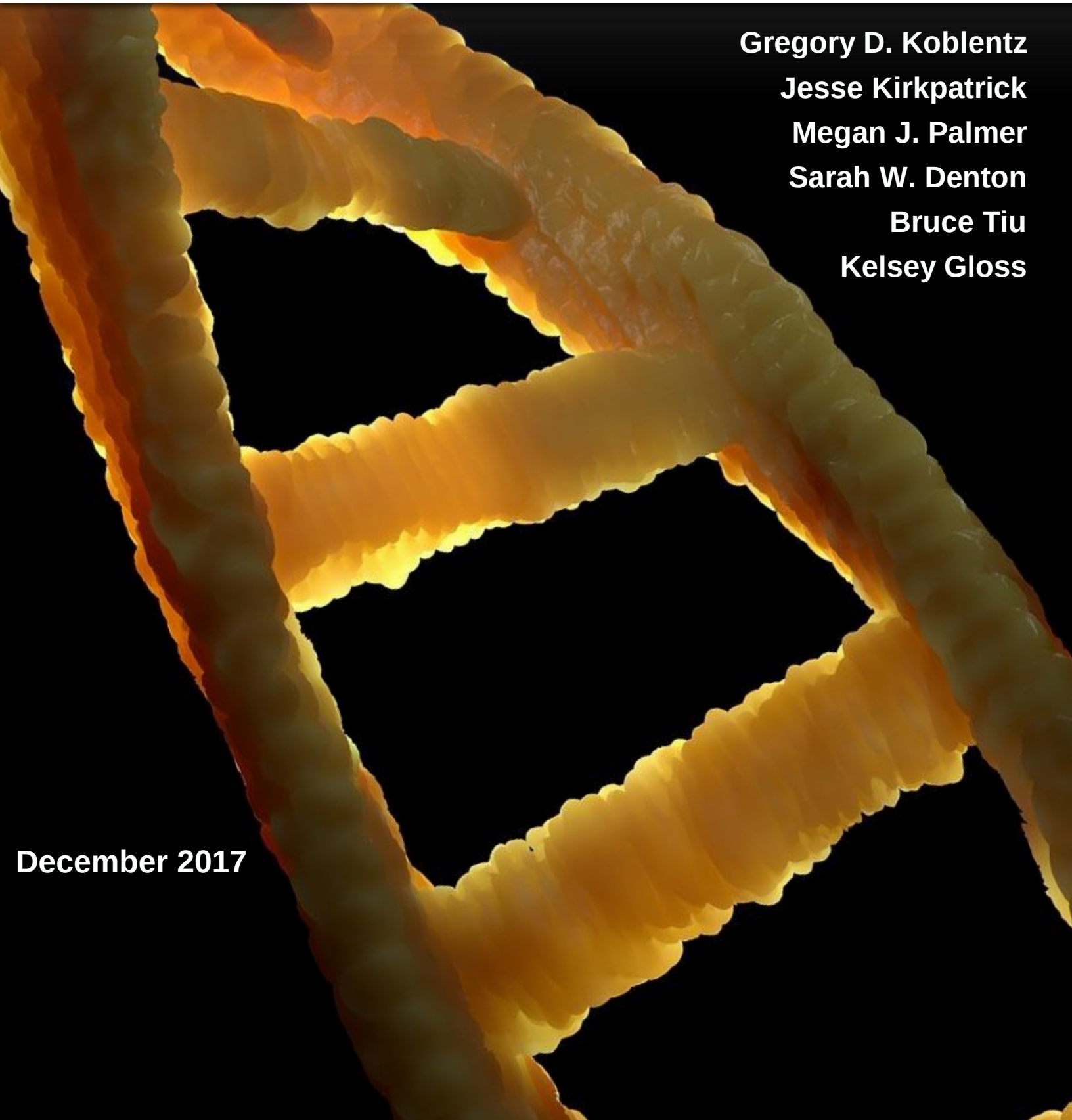
BIOTECHNOLOGY RISK ASSESSMENT: STATE OF THE FIELD

Editing Biosecurity Working Paper No. 1



Gregory D. Koblentz
Jesse Kirkpatrick
Megan J. Palmer
Sarah W. Denton
Bruce Tiu
Kelsey Gloss

December 2017

STUDY OVERVIEW

The rapid advancement of genome editing techniques, such as CRISPR, and its adoption by a broad range of users has sparked concerns that both state and non-state actors may seek to leverage peaceful advancements in genome editing for their own hostile purposes. Researchers from George Mason University and Stanford University initiated this two-year multidisciplinary study, *Editing Biosecurity*, to explore critical biosecurity issues related to CRISPR and related genome editing technologies. The overarching goal of this study is to present policy options and recommendations to key stakeholders. In the design of these options and recommendations, the research team focused on how to manage the often-competing demands of promoting innovation and preventing misuse, and how to adapt current, or create new, governance mechanisms to achieve these objectives.

The four study leads and and three research assistants for *Editing Biosecurity* were assisted by a core research group of fourteen subject-matter experts with backgrounds in the life sciences, industry, policy, ethics, and security. The centerpiece of the study were three invitation-only workshops that brought together the core research group for structured discussions of the benefits, risks, and governance options for genome editing. To support these workshops, the study leads prepared two working papers on risk assessment and governance and commissioned five issue briefs on key topics.

All of these working papers and issue briefs are available at the project's website: https://editingbiosecurity.org/.

A list of project participants can be found in the project's final report, *Editing Biosecurity: Needs and Strategies for Governing Genome Editing*, **which is available at: www.editingbiosecurity.org.**

CONTENTS

Scope of Work

This is the first section of a two-part working paper authored by the project's research team. The overall purpose of the working paper is to examine the state-of-the-art for assessing the risks and benefits of emerging dual-use technologies and examine how current policies used to govern dual-use technologies could be applied or adapted to genome editing technologies. This examination includes reflection on the utility of technology versus capability-based assessments. The working paper is intended to inform and guide discussion in the study's two workshops and lead directly into development of the study's white paper. Parts one and two of the working paper will be presented at workshops one and two, respectively.

Part One: Precedents in Technology Assessment--Part one of the working paper proceeds in two sections. Section one begins with a brief overview of security considerations related to genome editing. In this section we identify five areas of concern that have been the focus of analyses of the security implications of genome editing. Section two provides a brief overview of a selection of existing assessment and framework approaches that have been used to address security concerns related to emerging biotechnologies. The analysis of these existing approaches focuses on exploring similarities and differences in the respective studies' drivers, goals, scope, assumptions, and methodologies. The security considerations and selected studies in sections one and two, respectively, are intended to be illustrative, not exhaustive. The aim is to provide a representative sampling of key security concerns and previously developed technology frameworks and assessments. Security is often interpreted to mean a focus on national security. This project defines security more broadly to include national security, as well as security issues related to public health, the environment, and the economy. As a result of the high-level attention given to the potential for genome editing to be exploited for hostile purposes, this study will focus primarily, but not exclusively, on the risks associated with the deliberate misuse of these technologies. Since biosecurity overlaps with concerns about biosafety, biodiversity, the bioeconomy, and ethics, a holistic approach is necessary to ensure that policies designed to strengthen one area do not inadvertently weaken protections in another or that policies do not place unreasonably cumbersome limitations on innovative work in each area.

The overarching goal of this part of the working paper is to review the dominant security considerations, and the focus and methodologies of existing studies, in order to serve as a point of departure to consider how we can better assess this technology. We recognize that there are several areas worthy of attention that fall outside the present scope of part one of the working paper, including a comprehensive overview of the state of genome editing technology; the ethics of genome editing; and analyses of frameworks, assessments, and methodologies of technologies outside of the life sciences.

Part Two: A Guide to Governance Options for Genome Editing--Developed through the first workshop and in preparation for the second, the second section will examine past experiences developing and implementing options for governance of dual-use biotechnologies. This paper will review the existing biosafety and biosecurity regimes, propose lessons learned applicable to the governance of genome editing drawn from experiences including recombinant DNA, synthetic biology, dual-use research, and "gain of function" experiments, outline and evaluate existing proposals for governing genome editing, and explore new types of approaches to governance of this dual-use technology that are raised by the issue briefs and the first workshop.

Introduction to the Draft Framework: Parameters for Developing and Assessing Governance Options

Within the life sciences, some of the greatest advances have come in technologies that enable scientists to predictably and precisely modify the genomes of living organisms. These new techniques, such as the application of CRISPR (which stands for Clustered Regularly Interspaced Short Palindromic Repeats)-Cas, TALENS (which stands for Transcription Activator-Like Effector Nucleases), zinc finger nucleases, and meganucleases, are collectively known as genome editing. In 2012, a team of American and European researchers found that they could use proteins associated with an innate bacterial defense against invading viruses to make targeted cuts in DNA in bacteria and, in principle, in any organism.[1] In 2013, researchers at Harvard and MIT independently demonstrated the ability to leverage CRISPR to edit the DNA of eukaryotes such as mice and humans.[2] CRISPR-based techniques allow scientists to add, delete, or modify multiple genes simultaneously with a high degree of precision, in ways that are faster, cheaper, and easier to use than existing genetic engineering tools. By expanding the range of organisms that can be modified, the types of modifications that can be made, and the number of scientists and laboratories capable of making these modifications, genome editing is poised to make major contributions to life sciences research, medicine, public health, agriculture, and the biomanufacturing industry.

As with the case of recombinant DNA in the 1970s, and the emergence of synthetic biology in the 2000s, the rise of genome editing technologies, especially CRISPR, has raised hopes and fears about the impact on science, public health, medicine, the economy, and society. Although many of the risks and rewards under discussion today are the same ones featured during previous debates about recombinant DNA and synthetic biology, there are some notable differences. First, new genome editing technologies offer greater flexibility, precision, and versatility than previous approaches. These changes translate to both quantitative and qualitative differences in how genetic functions are targeted in a much wider array of platforms and potential application spaces. Moreover, developments in associated technologies including synthesis, automation, and screening combined with these functionalities means that the functional genetic landscapes can be explored more efficiently. The high rate of diffusion of these technologies also means that many more people are capable of exploring this landscape.

The Rise of CRISPR

Since 2012, CRISPR has diffused quickly and widely due to its versatility across a number of domains including scientific research, agriculture, human health, vector control, and biomanufacturing. For scientists, CRISPR has been used to control transcription, modify epigenomes, and conduct genome-wide screens and imaging chromosomes. CRISPR also allows

[1] Jinek M, et al., "A Programmable Dual-RNA–Guided DNA Endonuclease in Adaptive Bacterial Immunity," *Science* (2012 August 17); 337: pp. 816–821. doi: 10.1126/science.1225829; pmid: 22745249; and Gasiunas G., Barrangou R., Horvath P., Siksnys V. "Cas9- crRNA ribonucleoprotein complex mediates specific DNA cleavage for adaptive immunity in bacteria," *Proc. Natl. Acad. Sci.* (U.S.A. 2012 September 4); 109(39): pp. E2579–E2586 http://doi.org/10.1073/pnas.1208507109.

[2] Cong, L., Ran, F.A., Cox, D., Lin, S., Barretto, R., Habib, N., Hsu, P.D., Wu, X., Jiang, W., Marraffini, L.A., and Zhang, F. "Multiplex genome engineering using CRISPR/Cas systems," *Science* (2013 January 3); 339(6121), pp. 819–823 http://doi.org/10.1126/science.1231143; and Mali, P., Yang, L., Esvelt, K.M., Aach, J., Guell, M., DiCarlo, J.E., Norville, J.E., and Church, G.M. "RNA-guided human genome engineering via Cas9," *Science* (2013 January 3); 339(6121): pp. 823–826 http://doi.org/10.1126/science.1232033.

the targeting of several genes at once in order to study complex genetic processes or diseases caused by multiple mutations, something that could not be easily achieved previously. This feature enables researchers to better understand the functional organization of genomes at the systems level and the relationship between genotype and phenotype. While in the past, researchers have primarily relied on mice as a human model in genetic studies, the advent of CRISPR has also broadened the possibility of developing and conducting research in other animal models, such as pigs and primates. In the biomedical arena, CRISPR-based systems are being developed to remedy genetic disorders in humans, to treat cancer, and improve human resistance to diseases such as HIV. In addition to CRISPR-based somatic cell therapies, CRISPR has also been used experimentally to conduct germline editing in human embryos. In the medical field, CRISPR is also being used to engineer new antimicrobials, including antibiotics and antiviral drugs. In the field of agriculture, CRISPR is being adopted to accelerate the genetic engineering of plants and improve livestock breeding, which could lead to increased productivity and sustainability. CRISPR also has applications in the field of biomanufacturing by increasing the efficiency of industrial microorganisms and broadening the range of materials they are capable of producing, such as biofuels. Scientists have also used CRISPR to create gene drives capable of driving edited genes throughout a population via natural reproduction. The potential for editing genes to be "driven" through a population of fast-reproducing organisms (such as mosquitoes) has led to the exploration of using gene drives to control disease-carrying insects.[3]

Security Concerns Raised by Genome Editing

Genome editing is poised to make significant beneficial contributions in such areas as scientific research, agriculture, human health, vector control, and biomanufacturing. At the same time, members of defense, intelligence, and policy making communities have begun pondering the security implications of the rapid adoption of these technologies in laboratories around the world.[4]

In February 2016, Director of National Intelligence (DNI) James Clapper discussed genome editing in his annual worldwide threat assessment report to Congress. He warned, "Given the broad distribution, low cost, and accelerated pace of development of this dual-use technology, it's deliberate or unintentional misuse might lead to far-reaching economic and national security implications."[5] Genome editing was included among a list of six threats posed by weapons of mass destruction, and was the only biotechnology in the report's list, elevating this advance in research and development to a new level of concern. The subsequent DNI statement for the record, released in May 2017 under a new director, Dan Coats, omitted genome editing from the category of

[3] Barrangou B., Doudna JA. "Applications of CRISPR technologies in research and beyond," *Nature Biotechnology*. 2016 September; 34 (9): 933-941; and Hsu PD., Lander ES., Zhang F. "Development and Applications of CRISPR-Cas9 for Genome Engineering," *Cell* (2014 June 5); 157: pp. 1262-1278.

[4] Oye KA., Esvelt K., Appleton E., Catteruccia F., Church G., Kuiken T., *et. al.* "Regulating Gene Drives," *Science*, 2014 July 17. http://science.sciencemag.org/content/early/2014/07/16/science.1254287.full; Khan L., "A CRISPR Future," *Bulletin of the Atomic Scientist*, 2015 December 16. http://thebulletin.org/crispr-future8986; Gerstein DM., "How Genetic Editing Became a National Security Threat," *Bulletin of the Atomic Scientist*, (2016 April 25). http://thebulletin.org/how-genetic-editing-became-national-security-threat9362; and Jasanoff S., "CRISPR Democracy: Gene Editing and the Need for Inclusive Deliberation," *Issues in Science and Technology*, 2015; 32 (1), http://issues.org/32-1/crispr-democracy-gene-editing-and-the-need-for-inclusive-deliberation/.

[5] Director of National Intelligence, James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record to the Senate Armed Services Committee, (2016 February 9).

weapons of mass destruction. Instead, genome editing was categorized as one of four emerging and disruptive technologies that are considered "central to economic prosperity and social well-being, but...also introduc[ing] potential new threats."[6] DNI Coats went on to state, "Genome editing has the potential to cure diseases and modify human performance, which presents new ethical and security issues."[7]

Likewise, in June 2016, CIA Director John Brennan warned, "Nowhere are the stakes higher for our national security than in the field of biotechnology. Recent advances in genome editing that offer great potential for breakthroughs in public health are also cause for concern, because the same methods could be used to create genetically-engineered biological warfare agents. And though the overwhelming majority of nation states have tended to be rational enough to refrain from unleashing a menace with such unpredictable consequences, a subnational terrorist entity such as ISIL would have few compunctions in wielding such a weapon.[8] In October 2016, the United States warned members of the Biological Weapons Convention that "improvements to these gene editing/engineering technologies also increase the risk that weapons based on these technologies will be developed and used. Such technologies could be used to engineer modified or novel pathogens or toxins, but in principle it might also be possible to apply these technologies directly, for example by disrupting key RNA functions of humans, plants, or animals for hostile purposes. Periodically, concerns have been raised that it may become possible to develop weapons that are "selective" — that is, disproportionately likely to affect certain individuals based on their genetic makeup."[9] In November 2016, the President's Council of Advisors on Science and Technology identified advances in massively parallel DNA synthesis, improved knowledge of gene regulation, genome-editing technologies, and gene delivery as overcoming key obstacles that limited the utility of traditional genetic engineering for producing new and improved biological weapons.[10]

The rationale for the inclusion of genome editing in many of these assessments and statements is difficult to ascertain by virtue of the fact that they typically draw heavily from classified and restricted information. For example, the DNI's respective statements for the record exclude an articulation of such rationale from the *unclassified* publicly-released briefings to the Senate. Consequently, it is difficult to assess the validity of the rationale and assumptions that guide how decisions are made to highlight security considerations of genome editing.

Nevertheless, analyses of the security implications of genome editing has tended to focus on five sets of concern. First, and most commonly cited, is the relatively low cost and reported ease of using genome editing technology to modify organisms. Much of the commentary and media

---

[6] Director of National Intelligence, Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record to the Senate Armed Services Committee, (2017 May 11).
[7] Ibid. p. 4.
[8] Central Intelligence Agency Director John O. Brennan. Remarks at the Council on Foreign Relations, (Washington, DC, 2016 June 29), https://www.cia.gov/news-information/speechestestimony/2016-speeches-testimony/director-brennan-speaks-at-the-council-on-foreign-relations.html
[9] United States of America, "Article I: Reinforcing the core prohibition of the Biological Weapons Convention," Working Paper Submitted to the Eighth Review Conference of the States Parties to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, BWC/CONF.VIII/WP.14, (2016 October 25).
[10] President's Council of Advisors on Science and Technology, *Action Needed to Protect against Biological Attack* (Washington, DC: White House, November 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_biodefense_letter_report_fin.

reporting on risks associated with genome editing focus on how **the "democratization of biotechnology" will dramatically increase the number and type of individuals and groups capable of modifying pathogens to be more dangerous**.[11] This could entail endowing traditional biological warfare pathogens with enhanced properties such as increased infectivity, virulence, pathogenicity, and/or transmissibility; resistance to medical countermeasures; or the ability to avoid detection and diagnosis. Concerns over the accessibility of genome editing are accentuated by the rapid spread of this technology around the world (symbolized by China's early role in human gene editing research) and by the backdrop of escalating levels of violence committed by extremist non-state actors.

Second, there are also concerns that **genome editing could be used to create new types of biological weapons.** One type of novel bioweapon would be able to target specific biological systems (such as the cardiovascular, immunological, endocrine, neurological, reproductive, and gastrointestinal systems) and/or processes (such as metabolism, immune response, and homeostasis). For example, citing the potential for genome editing to "enhance (in vivo or in vitro) production of traditional or novel neurotoxins or infectious agents or to modify existing agents," Diane DiEuliis and James Giordano have warned, that "CRISPR-type gene editors could directly act on genes in the brain to alter neural phenotypes that influence cognition, emotion, and behavior."[12] Another type of novel bioweapon would enable an attacker to target a specific biological population based on unique genetic signatures at the individual or group level. John Sotos, chief medical officer of Intel, has speculated that advances in precision medicine, which depend on intimate knowledge of an individual's DNA in order to produce tailored therapies, will create the potential for biological weapons that can target specific individuals.[13] This risk was most vividly described by *The Atlantic* in an article titled "Hacking the President's DNA."[14]

Of special concern within this class of biosecurity risks would be the use of gene drives designed for controlling disease-carrying vectors such as mosquitoes to push deleterious genes into a population. According to Samuel Pope, "The possibilities for "weaponizing" gene drives range from suppressing pollinators, which could destroy an entire country's agriculture system, to giving innocuous insects the ability to carry diseases such as dengue."[15] Gene drives, according to

---

[11] Gerstein DM. "How Genetic Editing Became a National Security Threat," *Bulletin of the Atomic Scientists* [Internet] 2016 [cited 2017 October 13] https://thebulletin.org/how-genetic-editing-became-national-security-threat9362; and Gerstein DM, "Can the bioweapons convention survive Crispr?" *Bulletin of the Atomic Scientists* [Internet] 2016 [cited 2017 October 15] https://thebulletin.org/can-bioweapons-convention-survive-crispr9679; Loren Thompson, "Gene Wars: Targeted Mutations Will Spawn Unique Dangers, and Soon," *Forbes* [Internet] 2016 January 29 [cited on 2017 October 23], https://www.forbes.com/sites/lorenthompson/2016/01/29/gene-wars-targeted-mutations-will-spawn-unique-dangers-and-soon/#c4ce491786e7; Begley S, "Why the FBI and Pentagon are Afraid of this New Genetic Technology." *STAT News* [Internet] 2017, [cited on 2017], https://www.statnews.com/2015/11/12/gene-drive-bioterror-risk/.

[12] DiEuliis, D., Giordano, J. Why Gene Editors Like CRISPR/Cas May Be a Game-Changer for Neuroweapons. *Health Security*, 2017; *15*(3): pp. 296-302. doi:10.1089/hs.2016.0120.

[13] Jeffries A, ""Worse than death:" The far-future dystopia of genome hacking," *The Outline* [Internet], 2017 July 31, https://theoutline.com/post/2018/worse-than-death-br-the-far-future-dystopia-of-genome-hacking.

[14] Hessel A., Goodman M., Kotler S., "Hacking the President's DNA," *The Atlantic*, 2012 November , https://www.theatlantic.com/magazine/archive/2012/11/hacking-the-presidents-dna/309147/.

[15] Pope SM., "Impact of Gene Editing Tools, Like CRISPR/Cas9, on the Public Health Response to Disease Outbreaks," *Disaster Medicine and Public Health Preparedness*, 2016; 11(2): pp. 155-159.

Gabrielle Tarini and Raymond Zilinskas, "pose novel security risks for entomological warfare, agro-sabotage, and ecocide."[16]

Third, there is concern over using genome editing in humans, including both somatic cell and germline editing. One of the primary concerns involves the **potential use of genome editing to enhance warfighter capabilities**. A group of scientists in China edited the genome of non-viable human embryos in 2015,[17] and in 2017 a group of scientists in the U.S. made germline edits in embryos.[18] A number of technical hurdles remain, however, including off-target effects and mosaicism (when organisms contain a mix of edited and unedited cells). In addition, doubts persist over the claims of success made by some of these studies' authors.[19]

Furthermore, the use of germline edits for enhancing warfighters would require many years for the enhanced individuals to reach warfighting age, and there is considerable uncertainty that they would even make suitable soldiers after such a long period of time. This says nothing of the possibility for ethical and social opposition to using genome editing for the purpose of soldier enhancement. In combination, these factors make the feasibility and desirability of creating so-called "super soldiers" at present doubtful. Nevertheless, as James Clapper's 2016 comments indicate, there is clear concern over the possibility of "unregulated editing of the human germline...by countries with different regulatory or ethical standards than those of Western countries."[20] Should such enhancements come to fruition, they would likely provide military advantage on the battlefield. A worrisome security scenario for all militaries who seek to counter adversaries and terrorist groups.

A fourth concern is that **genome editing technology might cause harm accidently or inadvertently.** Many of these concerns relate to research and products that could be deliberately misused, but accidents that could lead to harm to researchers and/or the public could also occur (e.g. as was the case in "gain of function" studies where concerns about bioterrorism and biosafety failures leading to pandemic were of approximate equal magnitude). For example, one application of CRISPR is to use inhaled adenoviruses to introduce cancer-causing genes in mice in order to develop an animal model for human lung cancer. To mitigate the risk of this virus accidentally causing cancer in humans, this experiment used a RNA guide sequence that was unique to mice and a virus that was unable to replicate.[21] In another case, researchers who sought to make pigs resistant to foot and mouth disease virus used CRISPR to replace a pig's viral receptors with an analogous human receptor to which the virus would not recognize and bind. That type of experiment, however, runs the risk of creating conditions that favor the mutation of the virus to gain the ability to attach to these human-like receptors, which would also enable the virus to

---

[16] Tarini G., Zilinskas RA., "Gene Drives: Panacea or Pandora's Box?" [Internet] 2016 November 21 [cited on 2017 October 21], http://www.nti.org/analysis/articles/gene-drives-panacea-or-pandoras-box.

[17] Liang P., Xu Y., Zhang X., Ding C., Huang R., Zhang Z., *et al.* "CRISPR/Cas9-mediated gene editing in human tripronuclear zygotes." *Protein & cell*, 2015; 6 (5): pp. 363-372.

[18] Hong M., Marti-Gutierrez N., Park SP., Wu J., Lee Y., Suzuki K., Koski A., *et al.* "Correction of a pathogenic gene mutation in human embryos." *Nature* 2017; 548 (7668): pp. 413-419.

[19] Callaway E. "Doubts raised about CRISPR gene-editing study in human embryos," *Nature*, (2017 August 31); https://www.nature.com/news/doubts-raised-about-crispr-gene-editing-study-in-human-embryos1.22547; and Dieter E., Zuccaro M., Kosicki M., Church G., Bradley A., Jasin M. "Inter-homologue repair in fertilized human eggs?" *bioRxiv*, (2017 August 28); doi: https://doi.org/10.1101/181255.

[20] Director of National Intelligence, James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record to the Senate Armed Services Committee, (Washington, DC: 2016 February 9).

[21] Ledord H. "CRISPR, the Disruptor," *Nature*, 2015 June 4; 522: 21.

potentially infect humans as well.[22] Concerns have also been raised about the consequences of an accidental release of gene drives from a laboratory. As Sonia Ben Ouagrham-Gormley and Kathleen Vogel have pointed out, biosafety guidelines have not yet been developed for gene drive research "making it difficult for biosafety committees and scientists themselves to determine whether proper safety measures have been applied." [23] This concern is amplified by the democratization of biotechnology cited above, which potentially provides more powerful tools to DIYbio enthusiasts who do not necessarily have the knowledge or resources to implement appropriate biosafety protocols. In addition, given the lack of experience with gene drives and the complexity of ecosystems, there is a concern that gene drives released into the wild could unpredictably destabilize population dynamics, have an unintended impact on species not originally targeted by the gene drive, or have other ecological side effects.[24]

Finally, the DNI's stated concern over "far-reaching economic...implications" suggests that this may signal worry over **direct economic costs from an attack or security considerations stemming from a reduction in national economic competitiveness** due to another country gaining an edge in the bioeconomy. But as Kevin Esvelt and Piers Millett note, perhaps a larger animating concern for the U.S. intelligence community is **the possibility of countries using genome editing for enhancements and therapies for the *civilian* population.[25]** As they suggest, such economic advantages could be gained by reducing the prevalence of chronic health ailments or, in the longer term, increasing citizens' cognitive performance, both of which could have significant economic implications. The economic considerations they note are raised in the 2016 DNI report, and their assessment remains plausible to date as the DNI 2017 report states, "Genome editing has the potential to cure diseases and modify human performance, which presents new ethical and security issues."[26]

Despite these headline-grabbing concerns, others argue that currently there are **limitations on the ability of most actors to use genome editing to cause such harm, at least at present and in the near future.[27]** First, **moving from *in vitro* to *in vivo* applications of genome editing raises new challenges** such as molecular delivery to specific tissues or cells (via intramuscular injection, intravenous injection, or digestion absorption), maintaining the viability and stability of the molecule inside the organism, and the ability of the molecules to target and gain access to a cell in order to modify the targeted DNA.[28] Such technical barriers may limit, for example, the creation of "neuroweapons" or other 'personalized' bio weapons targeted at individual or group molecular

[22] Breaker R., (National Academies of Science, Engineering and Medicine workshop on Strategies for Identifying and Addressing Biodefense Vulnerabilities Posed by Synthetic Biology, Washington, DC) [Presentation] 2017 January 26.
[23] Ouagrham-Gormley SB., Vogel KM., "Gene Drives: the Good, the Bad, and the Hype," *Bulletin of the Atomic Scientists* [Internet] 2016, cited on 2017 October 23, https://thebulletin.org/gene-drives-good-bad-and-hype10027.
[24] Kenneth A. Oye. "Regulating Gene Drives," *Science*, 2014 July 17, http://science.sciencemag.org/content/early/2014/07/16/science.1254287.full.
[25] We recognize the difficulty in drawing a sharp distinction between enhancement and therapy.
[26] Director of National Intelligence, Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community," [Statement] (Record to the Senate Armed Services Committee, Washington), 2017 May 11.
[27] Spiez Laboratory, The Swiss Federal Institute for NBC-Protection, in collaboration with the Center for Security Studies-Swiss Federal Institute for Technology, *Spiez CONVERGENCE Report on the Second Workshop 5–8 September* (Federal Office for Civil Protection (FOCP), October 2016); Available at: https://www.labor-spiez.ch/pdf/en/Report_on_the_second_workshop-5-9_September_2016.pdf.
[28] Dieuliis, D., Giordano, J. Why Gene Editors Like CRISPR/Cas May Be a Game-Changer for Neuroweapons. *Health Security*, 2017;15(3): pp. 296-302.

signatures, and a similar set of challenges faces those who would develop and use gene drives for malicious purposes.[29] [30]

Second, several commentators argue that while the materials needed to conduct genome editing experiments are widely available, the **tacit knowledge and skills necessary to wield these tools effectively are much less common.** "The reality is that the techniques and expertise needed to create a deadly insect or virus are far beyond the capabilities of the typical DIY biologist or community lab...The materials might be available, but the knowledge and understanding needed to make edits that have the desired effects are not."[31] "Merely having access to materials, equipment, and even explicit knowledge is not sufficient—tacit knowledge and solutions to a host of social and organizational issues are also critically important."[8]

Third, even if genome editing made it much easier for less-skilled individuals to modify an organism, they would also need to overcome the **obstacles associated with growing the organism and disseminating it to cause mass casualties**. According to Todd Kuiken, "This would require additional skills and places CRISPR-based biological weapons beyond the reach of most terrorist groups."[32] Sonia Ben Ouagrham-Gormley and Kathleen Vogel similarly argue that "gene drives would seem to be beyond the capabilities of terrorists or biohackers with limited scientific knowledge and skills."[33] Such barriers indicate that at present there are easier paths for developing and delivering biological weapons.[34]

The full range of security concerns evoked by genome editing in general, and CRISPR in particular, has yet to be fully explored in a publicly available report. The emergence of CRISPR in 2012 sparked a number of studies on genome editing, but few of them address security concerns directly or deeply. The National Academies of Science, Engineering, and Medicine (NASM) has examined the ethical, social, and legal implications of genome editing in humans, but did not explore security considerations.[35] The NASEM culminating event on genome editing in humans, an international summit followed by commissioned papers, only began to scratch the surface of biosecurity issues. Charis Thompson underscored this absence in her commissioned paper where she listed biosecurity as one of the ten critically important, but missing, topics addressed by scholars who contributed to the International Summit.[36] The ecological risks associated with gene drives have been examined at great length in a report released in 2016 by the National Academies

[29] Ibid.
[30] Ouagrham-Gormley SB., Vogel KM., "Gene Drives: the Good, the Bad, and the Hype," *Bulletin of the Atomic Scientists* [Internet] 2016 [cited on 2017 October 23], https://thebulletin.org/gene-drives-good-bad-and-hype10027.
[31] Kuiken T. "Should We Fear DIY Biologists' Use of Cutting-Edge Gene-Editing Technology?" *Nature* [Internet] 2016 [cited on 2017 October 15] https://www.scientificamerican.com/article/should-we-fear-diy-biologists-use-of-cutting-edge-gene-editing-technology/
[32] Ibid.
[33] Sonia Ben Ouagrham-Gormley, Kathleen M. Vogel, "Gene Drives: the Good, the Bad, and the Hype," *Bulletin of the Atomic Scientists* (2016), accessed October 23, 2017, https://thebulletin.org/gene-drives-good-bad-and-hype10027
[34] Spiez Laboratory, The Swiss Federal Institute for NBC-Protection, in collaboration with the Center for Security Studies-Swiss Federal Institute for Technology, *Spiez CONVERGENCE Report on the Second Workshop 5–8 September* (Federal Office for Civil Protection (FOCP), October 2016); Available at: https://www.labor-spiez.ch/pdf/en/Report_on_the_second_workshop-5-9_September_2016.pdf: p. 24.
[35] United States National Academies of Sciences, Engineering, and Medicine (2016). – Human gene-editing initiative. Available at: www.nationalacademies.org/gene-editing/index.htm
[36] Charis Thompson, "Governance, Regulation, and Control: Public Participation," in *International Summit on Human Gene Editing: A Global Discussion*, (Washington, DC: U.S. National Academies of Science, 2016), http://nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_170455.pdf.

Committee on Gene Drive Research in Non-Human Organisms.[37] While the final NAS report on gene drives notes some biosecurity implications, the discussion is cursory and brief.

The first public risk assessment that addresses CRISPR and other genome editing technologies from the security perspective is being undertaken by NASEM as part of a broader assessment of synthetic biology and biosecurity. The preliminary risk assessment framework being developed by this NASEM committee is discussed in detail below. The 2017 NASEM report, which covered a broad range of technologies applicable to synthetic biology, including genome editing, noted that, "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."[38] Studies conducted by the JASON Federal advisory group in 2016 and by Gryphon Scientific remain classified or restricted.

Overview of Frameworks for Assessing the Risks of Dual-Use Biotechnologies

In this section, we begin by providing a brief overview of selected existing assessments and framework approaches that have been used to address security concerns related to emerging biotechnologies. The analysis of these existing approaches focuses on exploring similarities and differences in the respective studies' technologies considered, and the studies' drivers, goals, assumptions, and methodologies. This analysis is intended to be illustrative, not exhaustive.

Early Assessment Frameworks

Since the emergence of recombinant DNA technologies, there has been an abiding concern that advanced biotechnologies could be misused for hostile purposes. In a 1970 address to the Conference on Disarmament in Geneva, Nobel Laureate Joshua Lederberg anticipated the coming revolution in biology that would be unleashed by recombinant DNA as well as the potential dangers if these advances were applied to developing new and improved biological weapons.[39] During the 1980s and 1990s, assessments of the risks posed by rDNA focused on the ability of these tools to genetically engineer traditional biological warfare pathogens.[40] These studies were conditioned by several assumptions. First, it was assumed that the primary actors interested in developing biological weapons were states. Initially, this was a function of the Cold War and the widespread belief that the Soviet Union had a secret biological weapon. Later it was a function of the revelations of Iraq's pursuit of biological weapons and the UN's inability to verify the termination of that program. A second assumption was that these states were pursuing a deliberate

[37] U.S. National Academies of Science (NAS), *Gene Drive Research in Non-Human Organisms: Recommendations for Responsible Conduct* (Washington, DC: U.S. National Academies of Science, 2016), http://www.nap.edu/catalog/23405/gene-drives-on-the-horizon-advancing-science-navigating-uncertainty-and. pp. 159-162.
[38] National Academy of Science, Engineering, and Medicine (NASEM), A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology (Washington, DC: National Academies Press, 2017): p. 18.
[39] J. Lederberg, "Address to conference of the committee on disarmament, August 5, 1970," *Congressional Record*, September 11, 1970, p. 31395.
[40] Robert P. Kadlec and Alan P. Zelicoff, "Implications of the Biotechnology Revolution for Weapons Development and Arms Control," in Raymond Zilinskas, ed., *Biological Warfare: Modern Offense and Defense* (Boulder, CO: Lynne Reinner, 2000), pp. 11-26.

strategy to identify and apply rDNA techniques to achieve specific objectives, usually defined as militarily-useful attributes of biological weapons such as virulence, drug resistance, stability, ease of production, and the ability to evade detection and diagnosis.

Since 2001, assessing the security risks of advances in biotechnology changed in several ways. First, due to September 11th and the Amerithrax letters, there was a greater emphasis on terrorists as potential hostile actors. Most of these studies do not address the conditions under which terrorists would be interested in or capable of developing biological weapons or using advanced biotechnologies to do so. The existence of such groups is simply assumed without any analysis of their motivations or objectives. Second, due to the Australian mousepox experiment, which inadvertently demonstrated how to design an orthopox virus that could overcome vaccine-induced immunity, there was a greater emphasis on the potential for legitimate civilian research to be misused. Third, against a backdrop of globalization, these risk assessments are more sensitive to the pace of technological change and its degree of diffusion. In addition to examining the risks posed by specific tools and techniques, these studies also give almost as much weight to trends and trajectories of the technology. These studies, however, tend to fall into the trap of "technological determinism," which portrays the relentless advance of science and technology as an autonomous and inevitable process.

The major biotechnology risk assessment frameworks and studies published since 2000 share a common motivation born from an increased concern about the growing availability of increasingly powerful biotechnologies in a world where there are not enough restraints on the violent behavior of states and non-state actors.[41] These studies differ, however, in their scope, goals, and methodological and analytical approaches. Understanding the assumptions, strengths, and limitations of existing biotechnology risk assessments is an important first step to crafting improved frameworks for the characterization and assessment of technologies and options by which their development and (misuse) might be governed.

Biotechnology Research in an Age of Terrorism and Globalization: Biosecurity and the Future of the Life Sciences

Two early studies, *Biotechnology Research in an Age of Terrorism* (2004) and *Globalization, Biosecurity, and the Future of the Life Sciences* (2006), were conducted by the National Academies of Science.[42] *Biotechnology Research in an Age of Terrorism* (also known as the Fink Report after Dr. Gerald Fink the chair of the committee that wrote the report) was charged with reviewing U.S.

[41] Institute of Medicine and National Research Council, *Globalization, Biosecurity, and the Future of the Life Sciences* (Washington, DC: National Academies Press, 2006); Garfinkel MS, Endy D, Epstein GL, Friedman RM. "Synthetic genomics: options for governance," *Industrial Biotechnology*. 2007 Dec 1;3(4): pp. 333-65; Tucker, J.B. 2012. *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies*. Cambridge: The MIT Press; National Academy of Science, Engineering, and Medicine (NASEM), *A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology* (Washington, DC: National Academies Press, 2017); and Cummings CL, Kuzma J. Societal Risk Evaluation Scheme (SRES): scenario-based multi-criteria evaluation of synthetic biology applications. PloS one. 2017 Jan 4;12(1):e0168564.

[42] National Research Council (NRC), *Biotechnology Research in an Age of Terrorism*, (Washington, DC: National Academies Press, 2006); doi.org/10.17226/10827; Institute of Medicine and National Research Council (NRC), *Globalization, Biosecurity, and the Future of the Life Sciences* (Washington, DC: National Academies Press, 2006); doi.org/10.17226/11567.

policies and regulations designed to prevent destructive applications of biotechnology. While the report was motivated in part by the September 11th and Amerithrax terrorist attacks and recent examples of "contentious research," such as the previously cited mousepox experiment, it was also motivated by a recognition that the growing U.S. biodefense program would "inevitably create an increased number of research activities that raise concerns about misuse."[43] The report's most notable and enduring contribution to biotechnology risk assessment was the identification of seven "experiments of concern" that should be subject to review before they are carried out or published (see Table 1).

1. Would demonstrate how to render a vaccine ineffective.
2. Would confer resistance to therapeutically useful antibiotics or antiviral agents.
3. Would enhance the virulence of a pathogen or render a nonpathogen virulent.
4. Would increase transmissibility of a pathogen.
5. Would alter the host range of a pathogen.
6. Would enable the evasion of diagnostic/detection modalities.
7. Would enable the weaponization of a biological agent or toxin.

Table 1. The Fink Reports Experiments of Concern

The report, however, provided limited insight into how the committee developed these specific categories. The bulk of the report is devoted to a review of U.S. policies, regulations, and institutional processes to ensure the safe and secure conduct of life sciences research. The report briefly described several factors used to produce this list of experiments of concern: if the experiments were feasible with existing knowledge or technologies or with anticipated near-term advances, if the experiment represented a type of naturally occurring genetic change that could be replicated in a laboratory, if the experiment was associated with historical BW research, and/or if the experiment had the potential for causing serious harm without significantly improving our ability to defend against biological threats. The report acknowledged that its list was limited to microbial threats because it believed that self-replicating agents posed the greatest threat. Threats to humans, plants, and animals were considered. The report also recognized that advances in the life sciences would likely necessitate a revision to this list to encompass a broader range of biological threats in the future.[44] The report did not provide any meaningful guidance for how to assess the risks of specific experiments except that these judgments should be made by those with appropriate scientific expertise. Given the report's recognition of the "qualitative and case-by-case nature of these [types] of judgements," it also recommended that the review process for these types of experiments be administered by Institutional Biosafety Committees (IBCs) under the

[43] National Research Council (NRC), *Biotechnology Research in an Age of Terrorism*, (Washington, DC: National Academies Press, 2004); doi.org/10.17226/10827: p. 109.
[44] National Research Council (NRC), *Biotechnology Research in an Age of Terrorism*, (Washington, DC: National Academies Press, 2004); doi.org/10.17226/10827: pp. 113-114.

supervision of the National Institutes of Health (NIH) and its Recombinant DNA Advisory Committee (RAC). The Fink Report also recommended the creation of a National Science Advisory Board for Biodefense (NSABB), composed of scientists and national security experts, to provide advice on a wide range of issues associated with the conduct and oversight of dual-use research.[45]

The 2006 *Globalization, Biosecurity, and the Future of the Life Sciences* (also called the Lemon-Relman report after the co-chairs Drs. Stanley Lemon and David Relman) built on the Fink Report in several ways. First, while the Fink report was focused on research that could enhance the threats posed by infectious agents in the near-term, the Lemon-Relman report took a much broader and longer-term view of the biological threat landscape. The Lemon-Relman report assessed the impact of a variety of advances in the life sciences and biotechnology over the next five to ten years. The Lemon-Relman report devoted an entire chapter to describing a range of emerging biotechnologies, providing a much broader and deeper technical assessment than the Fink Report. In effect, the Lemon-Relman report shifted the biotechnology risk assessment paradigm away from discrete experiments to platform technologies that could be potentially misused in multiple ways. Second, the Lemon-Relman report was more strongly motivated by international trends in the development and diffusion of life science research and biotechnology than the Fink Report, which was more concerned with managing the increase in dual-use research on virulence and pathogenicity that was expected to result from the growing U.S. biodefense program. An entire chapter of the Lemon-Relman report was devoted to describing global drivers and trajectories of life sciences research and biotechnology. Third, the Lemon-Relman report had a wider aperture than that of the Fink report in terms of the types of risks about which it was concerned. This report explicitly includes not just deliberate and malevolent use of biotechnology by "smart and well-informed terrorists" but also the inappropriate use of biotechnology that could have unanticipated consequences if conducted with insufficient awareness or inadequate oversight.[46] In keeping with this broader framing of risk, the report defined biosecurity to include protection against inadvertent, inappropriate, or intentional malicious misuse of biotechnology.[47] The report does not explicitly describe the potential targets of biological threats, but the emphasis appears to be heavily weighted to human health as opposed to plants and animals.

[45] Ibid. pp. 115-120.
[46] Institute of Medicine and National Research Council (NRC), Globalization, Biosecurity, and the Future of the Life Sciences (Washington, DC: National Academies Press, 2006): pp. vii, 29.
[47] Ibid. p. 32.

Acquisition of Novel Biological or Molecular Diversity	Directed Design	Understanding and Manipulating Biological Systems	Production, Delivery, and Packaging
• DNA Synthesis • DNA Shuffling • Bioprospecting • Combinatorial Chemistry • High-Throughput Screening	• Rational Drug Design • Synthetic Biology • Genetic Engineering of Viruses	• RNA interference • High-Affinity Binding Reagents • Computational Biology and Bioinformatics • Systems Biology • Genomic Medicine • Modulators of Homeostatic Systems	• Biopharming • Microfluidics and Microfabrication • Nanotechnology • Aerosol Technology • Microencapsulation Technology • Gene Therapy • Targeting Biologically Active Molecules to Specific Locations in the Body

Table 2. Classification Scheme for Biological Technologies

One advantage of the Lemon-Relman report, in contrast to the Fink report, was that it moved away from a static, experiment-based approach to a more dynamic, technical capability-based perspective. The Lemon-Relman report does an impressive job of providing a *tour d'horizon* of emerging biotechnologies, including not only an assessment of the current state-of-the-art in each area but also future applications. A fundamental assumption of the report is that the rate of technical advances and diffusion is such that conducting a formal risk assessment of long-term biological threats posed by states and non-state actors would be an "exercise in futility."[48] Instead, the report categorizes these disparate technologies into four types of capabilities that they enable: acquisition of novel biological or molecular diversity, directed design, understanding and manipulation of biological systems, and production, delivery and packaging (see Table 2). These four categories are a useful conceptual framework for describing "the future threat landscape," but this rubric is not well-suited to navigating the threats and opportunities presented by that landscape.[49] Ultimately, the report does not provide a "process and set of organizing principles, a method by which technological advances might be assessed."[50] The process and method used in the report appear to rely heavily on the technical judgements of the scientific members of the committee who wrote the report. This is not to diminish their expertise or validity of their judgements, but this risk assessment methodology remains subjective, qualitative, and difficult to replicate consistently.

[48] Ibid. p. 18.
[49] Institute of Medicine and National Research Council (NRC), Globalization, Biosecurity, and the Future of the Life Sciences (Washington, DC: National Academies Press, 2006): p. 18.
[50] Ibid. p. viii.

The Lemon-Relman approach to biotechnology risk assessment directly informed one of their major policy recommendations. Unlike the Fink report that was heavily focused on institutional oversight within the United States, the Lemon-Relman report focused on international threats from states and terrorists enabled by advanced biotechnology. Recognizing that assessing these types of threats requires both access to intelligence on potential adversaries and scientific expertise drawn from multiple fields, the report emphasized the need to empower national security agencies (including the intelligence community) with the expertise and networks to conduct their own risk assessments of the sort carried out by this report.[51]

Synthetic Genomics: Options for Governance

Subsequent studies have tended to be narrower in scope, focusing on specific technologies or governance strategies. The 2007 *Synthetic Genomics: Options for Governance* report by the J. Craig Venter Institute (JCVI), Center for Strategic and International Studies (CSIS), and MIT explored the biosafety and biosecurity risks posed by the creation of synthetic pathogenic microorganisms. Specifically, the report considered the impact of synthetic genomics on three key issues: bioterrorism, worker safety, and the protection of communities and the environment.[52] The report specifically excluded the risks posed by state-sponsored biological warfare programs. The stated rationale for this exclusion was the belief that remediating such state-sponsored activity is best achieved at the governmental level, either state-to-state or collectively, which was beyond the study's scope.[53] The report's treatment of the benefits of synthetic biology was a broad qualitative overview of the potential contributions that synthetic genomics can make in areas such as basic research, human and animal vaccines, new or improved drugs, and biomanufacturing. The foundation of the report's analysis of the safety and security risks posed by synthetic genomics was provided by commissioned papers written by two virologists who were asked to assess the ease or difficulty of synthesizing a long list of pathogenic viruses, and to compare that process to the ease or difficulty of obtaining that virus by other means. These papers were supplemented by three workshops and a larger meeting to solicit input from a wide range of experts. The centerpiece of the report's risk assessment was a table rank-ordering important pathogenic viruses in terms of the difficulty of synthesizing the virus, assuming that an individual has knowledge of and experience in virology and molecular biology and an equipped lab, but not necessarily with advanced microbiological experience. This assessment was based on a consensus of the virologists and molecular biologists who participated in the study. In addition, the report considered how the evolution of synthetic biology would affect risks during the near-term (within the next five years) and longer term (10+ years). Over the near-term, the primary concern was the synthesis of a small number of highly pathogenic viruses that are otherwise difficult to obtain. Over the long-term, it was believed that it would be easier to synthesize viruses of any size than obtain them through other means. In addition, anticipated advances in synthetic genomics would also make possible the synthesis of bacterial pathogens and the construction of new microorganisms based on novel DNA sequences.

[51] Ibid. pp. 236-243.
[52] Garfinkel MS, Endy D, Epstein GL, Friedman RM. "Synthetic genomics: options for governance," *Industrial Biotechnology.* 2007 Dec 1;3(4): pp. 333-65.
[53] Ibid. p. 9.

Based on this risk assessment, the report offers multiple options for policies that could be developed by or applied to three key groups, commercial firms that sell synthetic DNA, owners of desktop DNA synthesizers, and the scientists and institutions that use synthetic DNA, to reduce the risks of deliberate or accidental incidents. The report is agnostic about whether these options are adopted voluntarily or imposed by legislation, regulation, or policy. Each option is also judged based on its feasibility and desirability using the following governance goal criteria:

- Does the option hold down costs and other burdens to both government and the affected industry?
- Can the option be implemented today, or is additional research required before it will be effective?
- Does the option unduly impede biological research or progress by the biotechnology industry?
- Does the option help to promote constructive applications of the technology?
- Is the option scalable or transferrable to be implemented internationally?
- Will the option be able to keep pace with evolving science and technology?

Table 3. Criteria for Evaluating Feasibility and Desirability of Governance Options

The report is notable for the transparency of its risk assessment process and for the detailed assessment of different governance options.

Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies

In the 2012 book, *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies*, Jonathan B. Tucker provided a decision framework for assessing the risks and governability of emerging dual-use technologies (see Figure 1).[54] Within this framework, assessments of the risk of misuse were based on four parameters: accessibility, ease of misuse, magnitude of potential harm, and imminence of misuse. The overall risk of misuse was based on the average of a three-level ordinal scale (low, medium, and high) for each variable. Like many of the other studies examined so far (and detailed below in the section, Reflections of Biotechnology Risk Assessments), Tucker addresses the issue of intent by presuming the existence of state and non-state actors with malign intent.

A major strength of this decision framework is that it was applied by other experts to a range of chemical and biological technologies. Based on these case studies, Tucker found that the aggregate risk score was a good indicator of whether or not a technology posed a significant risk of misuse. Technologies with a high aggregate score meant that the technology had significant potential for large-scale harm in the near future while technologies with a low score were either incapable of causing large-scale harm or their ability to do so was in the distant future. The variables in this

[54] Jonathan B. Tucker, ed., Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies (Cambridge: MIT Press, 2012

framework, therefore, have been validated across a range of cases which provides confidence that this framework can be applied to other technologies.

An important strength of Tucker's decision framework is that it also includes a mechanism for evaluating the governability of a technology. Tucker identifies five key parameters for determining the governability of a technology: embodiment, maturity, convergence, rate of advance, and international diffusion. Each variable would be scored on a three-level ordinal scale and the governability of a technology would be based on its average score.

The final portion of Tucker's decision framework combines the risk assessment and level of governability to select an appropriate package of governance measures that will minimize the risks posed by the technology while not sacrificing the benefits it promises. This final step is accomplished by performing a cost-benefit analysis that takes into account the anticipated benefits of the technology, the direct and indirect costs of the proposed governance measures, and the attitudes of stakeholders that may be affected by the proposed policies. This component of Tucker's decision framework remains a black box, a recognition that this type of cost-benefit analysis would be highly political and subject to a range of non-rational factors.

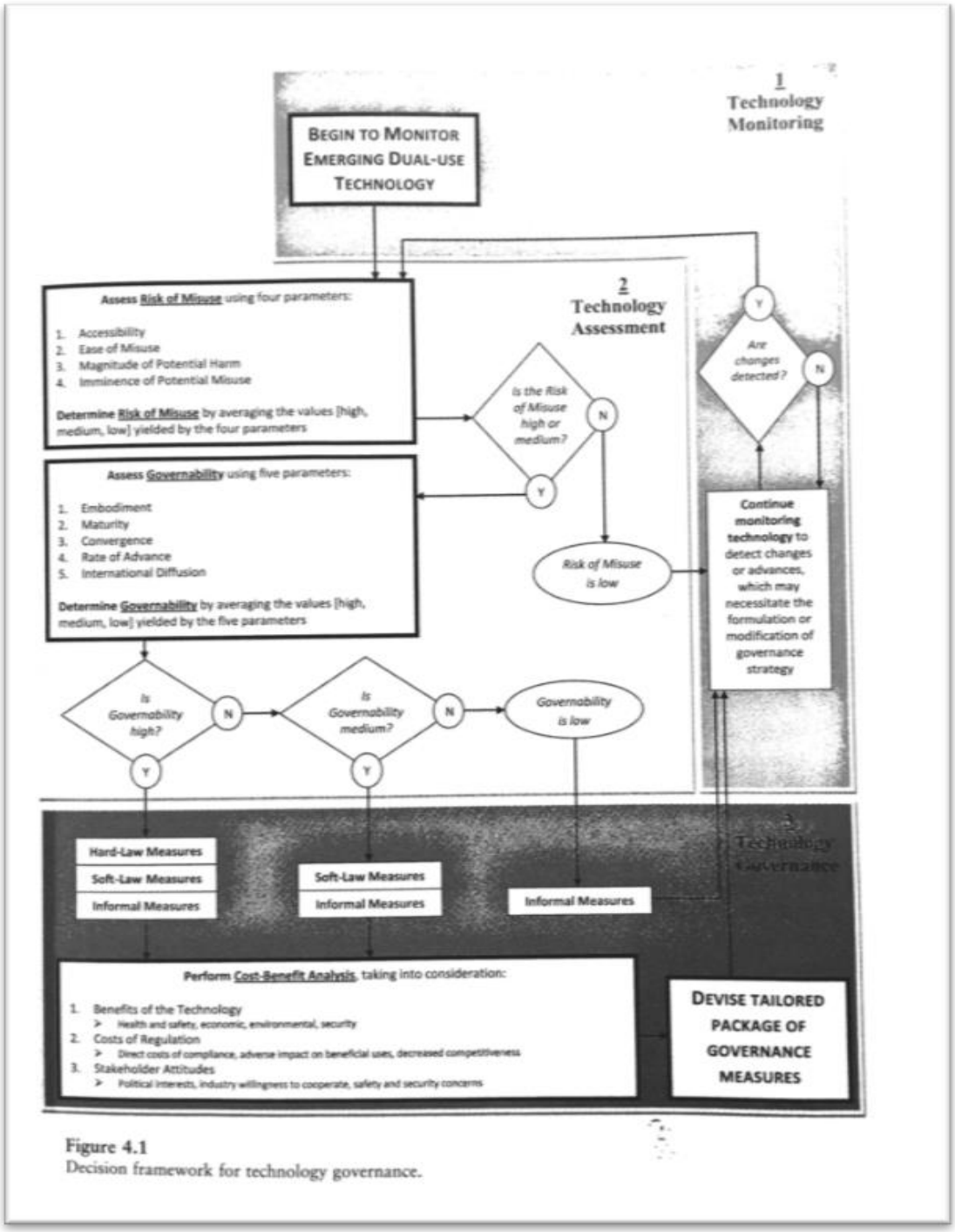


Figure 4.1
Decision framework for technology governance.

Figure 1. Tucker's Decision Framework for Assessing the Risk and Governability of Dual-Use Technology

Risk and Benefit Analysis of Gain of Function Research

As part of the "deliberative process" initiated by the White House in 2014 to develop a policy for governing "gain of function" (GOF) experiments that could generate pathogens with pandemic potential (PPP), NSABB commissioned a report by Gryphon Scientific to assess the risks and benefits of these types of experiments. The NSABB defined gain-of-function research of concern (GOFRC) as "research that can be reasonably anticipated to generate a pathogen with pandemic potential. Determining whether a proposed research project is likely to do so will entail uncertainty and will require scientific and other expert judgment."[55] The authors acknowledged that the term "gain-of-function" (GOF) has been criticized by both proponents and critics of GOF research for being too broad and not descriptive enough, but they failed to offer a narrowed definition.[56] Gryphon published its final report, *Risk and Benefit Analysis of Gain of Function Research* [hereafter RBA], in April 2016.[57] The RBA focused on GOF studies with influenza viruses and the coronaviruses that cause SARS and MERS since these were designated by the White House as pathogens with pandemic potential (PPP). The RBA defined risk in an actuarial sense as a function of the probability of an event occurring and its consequences. The RBA was designed to assess the risk that GOF research would either increase the probability that an outbreak involving a PPP would occur and/or increase the consequences of such an outbreak. The report analyzed the safety risks and security risks posed by GOF experiments separately.

The safety risks were evaluated using "sophisticated quantitative modeling of the probability and consequences of various events that lead to an outbreak, the ongoing transmission of the outbreak in humans, and the termination of the outbreak by public health measures or natural forces."[58] A combination of Fault Tree Analysis (FTA) and Probabilistic Risk Assessment (PRA) was used to estimate the safety risks of GOF research. FTA was used to estimate the likelihood of a particular type of safety failure occurring and PRA was used to estimate the frequency and magnitude of an outbreak resulting from such failures. The goal was to estimate both the likelihood and consequences of an accident involving a pathogen with enhanced properties. To do so, the RBA evaluated the potential of specific types of modified phenotypes including those with enhanced production, enhanced morbidity and mortality, enhanced transmission in mammals, altered host range, evasion of existing natural or induced immunity, and resistance to drugs or evasion of other medical countermeasures, to cause a global pandemic. Thus, the GOF experiments of concern were similar to, but not identical to, the "experiments of concern" described in the Fink Report. To estimate the likelihood of an accidental release of an enhanced pathogen, the safety assessment estimated the role of such laboratory features and practices as containment features, personal protective equipment, decontamination procedures, incident reporting, and occupational health on biosafety. A key finding was that human error was by far a more likely cause of a biosafety failure than mechanical error, but knowledge of the rates and causes of such failures was judged to be

[55] National Science Advisory Board for Biosecurity (NSABB) 2016, Recommendations for the Evaluation and Oversight of Proposed Gain-of-Function Research, (National Institutes of Health: Office of Science Policy, 2016): p. 41
[56] Ibid. p. 67.
[57] Gryphon Scientific, *Risk and Benefit Analysis of Gain of Function Research: Final Report* (April 2016); Available at: http://www.gryphonscientific.com/wp-content/uploads/2016/04/Risk-and-Benefit-Analysis-of-Gain-of-Function-Research-Final-Report.pdf
[58] Ibid. p. 1.

inadequate. In addition, the safety assessment discussed, but did not include in the parametric analysis, intangible factors associated with biosafety such as training and education, laboratory management, and institutional culture.

The security risk assessment examined the risks posed by the intentional release of an enhanced pathogen as well as the risks posed by the publication of GOF research. The first part of the security risk assessment was based on a review of past malicious incidents involving biomedical laboratories or pathogens and an evaluation of current security measures in place. The RBA judged that the most likely route to a deliberate release of an enhanced pathogen capable of causing a global pandemic was an insider who misuses their access to the laboratory. The RBA also assessed the degree to which additional GOF research would provide a malicious actor with further knowledge that could be used to create their own enhanced pathogen. The report concluded that given the extensive amount of information in the public domain on how to grow and modify influenza viruses, further GOF experiments would not pose an increased information risk. A significant information security risk remains for GOF experiments that could demonstrate how to produce a more transmissible strain of coronavirus while maintaining its natural level of pathogenicity.

Finally, the report analyzed the potential benefits of GOF research with influenza and coronaviruses. This analysis compared the scientific knowledge expected to be gained from such research with known gaps in our understanding of these pathogens and weaknesses in relevant medical and public health capabilities, alternatives to achieving these benefits with different experimental approaches, and scientific or technical innovations that could provide similar benefits through completely different mechanisms. Whereas the biosafety and biosecurity risk assessments were quantitative and semi-quantitative respectively, the benefits assessment was qualitative. The report found that GOF research with influenza and coronaviruses provided many unique benefits to studying these viruses although in some cases the same results could be achieved with alternative methods. To compensate for the mismatch between immediate risks and future benefits that is common to assessments of dual-use research, the report also identified the scientific and non-scientific barriers that may prevent or delay the realization of the benefits offered by GOF research. The report also sought to determine the extent to which the risks and benefits of GOF research are equally distributed across populations.

The RBA utilized a five-year time horizon for assessing risks, while benefits were assessed over a longer timeframe. The RBA was notable for its extensive data collection, rigorous methodology, use of multiple methodologies, transparency regarding its data and analysis, comparative approach to risk assessment, and evaluation of the benefits provided by GOF research. While the scope of the report, analyzing the impact of GOF research with influenza and coronaviruses, was narrow within the context of dual-use research, it covered this topic in a very comprehensive manner. The parametric approach to assessing safety risks provides a useful framework for evaluating the impact of different phenotypes and laboratory features and practices on the relative biosafety risks associated with GOF experiments. At the same time, the report underscored large gaps in our knowledge about the causes and consequences of both disease outbreaks and biosafety and biosecurity failures. Due to these gaps, a good deal of uncertainty remains regarding the absolute risks of a biosafety or biosecurity failure that results in the release of an enhanced pathogen that can cause a global pandemic. However, the overall assessment concluded that the biosafety and biosecurity risks are of the same order of magnitude.

A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology

In 2016, the National Academies of Science launched another major effort to assess the risks posed by emerging biotechnologies, this time with a focus on the field of synthetic biology. In 2017, the Committee on Strategies for Identifying and Addressing Biodefense Vulnerabilities Posed by Synthetic Biology released a preliminary report titled, *A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology*.[59] The committee examined the security considerations posed by synthetic biology to human health and the ability of military personnel to execute their missions. The committee included the modification of organisms to alter the environment or materials only to the extent to which they directly affected warfighters. Synthetic biology was broadly defined to include "the manipulation of biological functions, systems, or microorganisms resulting in the production of a disease-causing agent or toxin."[60] Likewise, the definition of "agent" was broadly defined to include pathogens, toxins, "or even a biological component, such as a genetic construct or biochemical pathway" that could be used to cause harm to humans.[61] This broad scope of what constitutes a biological threat is in keeping with the framing offered by the Lemon-Relman report. This study purposefully excluded the consideration of benefits from its scope.

The goal of the study was to provide "a framework for considering the types of malicious actions that could conceivably be taken and assessing the degree of concern that might be warranted."[62] To achieve its first goal, the report uses the Design-Build-Test concept, an iterative description of the product development process that the synthetic biology community imported from the engineering world, as its framework for categorizing a range of synthetic biology technologies and applications (see Table 4). This is similar in purpose to the four-fold classification scheme used in the Lemon-Relman report in 2006, although their expanded framework emphasized how technologies can contribute to multiple stages of the engineering process. This report excludes the consideration of intent from its analysis since the authors did not have access to intelligence on actors that might be interested in using this technology to cause harm and if so how they plan on doing so. Likewise, the study eschews the use of the term risk since the term connotes knowledge of the likelihood and severity of harm, but without information about the intent of actors to misuse this technology it is not possible to provide a reliable estimate of likelihood.

[59] National Academy of Science, Engineering, and Medicine (NASEM), A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology (Washington, DC: National Academies Press, 2017).
[60] Ibid. p. 5.
[61] Ibid.
[62] Ibid. p. 6.

Design	Build	Test
• Automated Biological Design • Metabolic Engineering • Phenotype Engineering • Horizontal Transfer and Transmissibility • Xenobiology • Human Modulation • Directed Evolution	• Automated Biological Design • DNA Construction • Editing of Genes or Genomes • Library Construction • Booting of Engineered Constructs • Directed Evolution	• High-Throughput Screening • Directed Evolution

Table 4. Design-Build-Test Framework for Assessing Risks of Synthetic Biology Technologies

The report also provided a list of factors to assess the degree of concern with particular synthetic biology tools and technologies. This list was based on a combination of factors that reflect the capability of a malicious actor to use the technology to cause harm and the capability of a defender to mitigate the effects of such an attempt (see Table 5). The report provided a comprehensive menu of factors that could affect the ability of a malicious actor to use synthetic biology to cause harm. The factors include both material considerations and intangible factors such as expertise. Although the factors largely parallel the ones developed by Tucker, the committee provides more technical guidance than Tucker did on how to score these technologies on the different parameters. The description of each variable is accompanied by a number of questions that can be used to qualitatively score the technology on an ordinal scale. This framework is also the only one that includes an analysis of capabilities that can be used to mitigate the risks it is assessing. One factor that might complicate an assessment of mitigation capabilities is identifying capabilities that are uniquely suited for countering threats enabled by synthetic biology versus capabilities that are needed to respond to naturally occurring infectious disease outbreaks or attacks with unmodified pathogens or toxins.

The next phase of the study will apply these factors to the designated synthetic biology technologies in order to determine the degree of concern that each one poses. The report is admirably frank about the utility and the limitations of its framework. Despite these limitations, the framework has the potential to be applicable to a wide range of biotechnologies, not just those covered in the report, and to enable long-term monitoring of technologies to determine if new advances change the degree of concern associated with the technology. On the other hand, while the framework provides a comprehensive list of factors to consider, it does not provide a methodology for identifying and collecting the necessary information, analytical techniques to convert this information into a meaningful degree of concern, or a methodology for weighing the relative importance of the different factors. Instead, the committee recognizes that making judgements about the degree of concern posed by a technology or combination of technologies will rely on the scientific expertise of the assessors, using primarily qualitative data and methods.

Factors to Assess Capability for Malicious Use	Factors to Assess Capability for Mitigation
Use of Technology • Ease of Use • Rate of Development • Barriers to Use • Synergy • Cost Use as a Weapon • Production and Delivery • Scope of Casualty • Predictability of Results Attributes of Actors • Access to Expertise • Access to Resources • Organizational Footprint Requirements	Deterrence and Prevention Capabilities Capability to Recognize an Attack Attribution Capabilities Consequence Management Capabilities

Table 5. Factors for Assessing Degree of Concern

Reflections on Biotechnological Risk Assessments

In summary, the differences in drivers, goals, and technologies considered, the variable treatment of intent, risks, and benefits, and the different time horizons selected by these different assessments all contributed to varying points of departure for existing studies. Moreover, a number of additional decisions further impact the design and construction of the respective studies' frameworks and assessments. For example, the 2006 and 2017 NASEM studies organize their analyses around categories of technologies that have similar applications. The 2006 report categorized then-recent advances into four categories according to "common purposes, common conceptual underpinnings, and common technical enabling platforms."[63] This conceptual framework was favored over a risk assessment because it was believed to have the advantage of providing a broader avenue of analysis of threats, and a greater likelihood of not being rendered irrelevant by the fast pace of scientific advances.[64] The 2017 NASEM committee took a similar approach using the Design-Build-Test rubric as their organizing principle for categorizing synthetic biology technologies.[65]

Instead of focusing on a suite of technologies, other studies employed an in-depth case study approach.[66] For example, Tucker developed his governance framework through an iterative process of deductive reasoning and analysis of empirical case studies.[67] Others too have used iterative case studies in their analyses of gene drives.[68] The criteria used to select the cases include the plausibility that the organism(s) selected in the case(s) was suitable for gene drive modification and the likelihood that the research or application would be conducted or pursued in the near future. In addition, the study sought to present a diversity of cases ranging from target organisms, applications, and location of research and release.[69] The Gryphon Scientific RBA is notable for its use of multiple quantitative and qualitative methodologies and the level of detail provided regarding its analytical methods and sources of data.

Making predictions about the trajectory of emerging technologies is notoriously difficult. Typically, the accuracy of predictions functions in inverse proportion to the length of the time horizon. Consequently, many frameworks and assessments limit the time horizon to the near to

[63] Institute of Medicine and National Research Council (NRC), Globalization, Biosecurity, and the Future of the Life Sciences (Washington, DC: National Academies Press, 2006): pp. 141-142.
[64] Ibid. pp. 3, 18.
[65] National Academy of Science, Engineering, and Medicine (NASEM), A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology (Washington, DC: National Academies Press, 2017): p. 5.
[66] Jonathan B. Tucker, ed., *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies* (Cambridge: MIT Press, 2012). U.S. National Academies of Science, *Gene Drive Research in Non-Human Organisms: Recommendations for Responsible Conduct* (Washington, DC: U.S. National Academies of Science, 2016), http://www.nap.edu/catalog/23405/gene-drives-on-the-horizon-advancing-science-navigating-uncertainty-and.
[67] Ibid. p. 67.
[68] U.S. National Academies of Science (NAS), *Gene Drive Research in Non-Human Organisms: Recommendations for Responsible Conduct* (Washington, DC: U.S. National Academies of Science, 2016), http://www.nap.edu/catalog/23405/gene-drives-on-the-horizon-advancing-science-navigating-uncertainty-and
[69] Ibid. p. 49.

mid-term of 5-10 years.[70] Some studies opt to focus on the near (today), mid (up to five years) and long-term (more than 5 years).[71] Others scan further on the horizon: up to 50 years.[72]

Risk & Intent

In non-technical, colloquial usage, risk typically refers to instances in which an unwanted outcome is possible. With respect to emerging technologies, risks are often uncertain. Such uncertainty can manifest with respect to outcomes (i.e., the outcome is unknown, as may be the case with technologies or products for which there are few or no comparators),[73] or in cases where the outcomes are known but the probabilities are not.[74]

Within the context of biosecurity and biosafety, the term risk is defined in various ways. For example, risk is often defined as "the likelihood and severity of harm."[75] Some studies have chosen to also include in their conception of risk how the given risk(s) occur(s) in pathways.[76] Some scholars take a broader conception of risk. With respect to gene drives, ecological risk has been defined as the probability of an agent or actor, that has the potential to alter a component of the ecosystem, which can impact endpoints—values that need to be managed or protected—such as societal, human health, or environmental values.[77] In an even broader construal of risk, some scholars have opted to broaden the conception of risk beyond the "technical definition of the severity of the hazard combined with the likelihood of occurrence or exposure" to include psychometric and social factors that affect risk perception and risk management such as the degree

---

[70] Institute of Medicine and National Research Council (NRC), *Globalization, Biosecurity, and the Future of the Life Sciences* (Washington, DC: National Academies Press, 2006); Garfinkel MS, Endy D, Epstein GL, Friedman RM. "Synthetic genomics: options for governance," *Industrial Biotechnology*. 2007 Dec 1;3(4): p. 13; National Academies of Sciences, Engineering, and Medicine (NASEM), 2017. *Preparing for Future Products of Biotechnology*. (Washington, DC: The National Academies Press, 2017); Available at: https://doi.org/10.17226/24605: p. ix.

[71] National Academy of Science, Engineering, and Medicine (NASEM), A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology (Washington, DC: National Academies Press, 2017), p. 9.

[72] Cummings CL, Kuzma J. Societal Risk Evaluation Scheme (SRES): scenario-based multi-criteria evaluation of synthetic biology applications. PloS one. 2017 Jan 4(12); 1:e0168564**:** p. 5.

[73] For such claims about synthetic biology see Denise Caruso, *Synthetic Biology: An Overview and Recommendations for Anticipating and Addressing Emerging Risks*, (Washington, DC: Center for American Progress, November 2008), Available at: https://www.scienceprogress.org/wp-content/uploads/2008/11/syntheticbiology.pdf: p. 10. For products without comparators see National Academy of Science, Engineering and Medicine, *Preparing for Future Products of Biotechnology*. (Washington, DC: The National Academies Press, 2017) doi: 10.17226/24605. p. 110-112.

[74] See Cummings CL, Kuzma J. Societal Risk Evaluation Scheme (SRES): scenario-based multi-criteria evaluation of synthetic biology applications. PloS one. 2017 Jan 4;12(1):e0168564. Uncertainty is defined as including both "unknown-ness and unfamiliarity" and "uncontrollability." pp. 13-17.

[75] National Academy of Science, Engineering and Medicine, *Preparing for Future Products of Biotechnology*. (Washington, DC: The National Academies Press, 2017) doi: 10.17226/24605. p. 6. See also Cummings CL, Kuzma J. Societal Risk Evaluation Scheme (SRES): scenario-based multi-criteria evaluation of synthetic biology applications. PloS one. 2017 Jan 4;12(1):e0168564. p. 8.; and National Academies of Sciences, Engineering, and Medicine, *Dual Use Research of Concern in the Life Sciences: Current Issues and Controversies.* (Washington, DC: The National Academies Press, 2017) doi: https://doi.org/10.17226/24761: p. 11.

[76] Renn, O. 1992. "Concepts of risk: A classification" pp. 53–79 in Social Theories of Risk, S. Krimsky and D. Golding, eds. Westport, CT: Praeger. As cited in, National Academy of Science, Engineering, and Medicine, *A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology* (Washington, DC: National Academies Press, 2017): p. 65.

[77] National Academy of Science, Engineering and Medicine, *Preparing for Future Products of Biotechnology*. (Washington, DC: The National Academies Press, 2017) doi: 10.17226/24605; and National Academies of Science, Engineering, and Medicine, *Gene Drives on Horizon*, (Washington, DC: The National Academies Press, 2016) doi: 10.17226/23405; Available at: https://www.gene-drives.com/gene-drives.pdf: pp. 22, 113.

of unmanageability, irreversibility, and public concern of potential hazards.[78] Cummings and Kuzma prefer the term ***societal risk*** as it includes "psychometric and social factors that affect how people perceive risk and what they place value upon in preventing, mitigating, or accepting risk."[79]

Risks arising from genome editing could be the result of an accidental release of a modified organism or pathogen, unanticipated consequences of a laboratory or field experiment, or malicious misuse of the technology by a terrorist group, non-state actor, or government. Such risks represent a spectrum of actions in which intent plays a pivotal role; they range from harms resulting from a lack of intent (pure accidents) to reckless intent (accidents due to negligent or irresponsible behavior) to malicious intent (deliberate efforts to cause harm). Since they are in a direct relationship, the role of an actor's intent is a critical factor in assessing the likelihood of risk with respect to malicious misuse. Not unlike the risk of malicious misuse, *threat* also requires intent. In order to adequately assess a particular threat, one must have knowledge of both the actor's intent and the capabilities of the actor.[80] Capability can be understood as the power or ability of an actor to access or use a technology.

Treatment of the relationship between threat, intent, and risk, with respect to malicious misuse, has varied among these frameworks and assessments. Some scholars treat mal-intent as a constant in their approaches to risk assessment. For example, in his decision-framework, Tucker acknowledges the difficulty in predicting intent, and, therefore, assumes that certain actors possess constant malign intent and are continuously searching for ways in which it can be exercised.[81] Consequently, in the absence of access to classified intelligence, Tucker concluded that intent must be excluded as a variable in his framework.

The NASEM Committee on Strategies for Identifying and Addressing Biodefense Vulnerabilities Posed by Synthetic Biology was also explicit in its rationale for focusing on the capabilities of actors in their framework, and not risks or threats. Since the Committee did not have access to classified intelligence, which would have provided insight into the motivations of actors, it asserted that it could neither estimate the likelihood of harm (risk) nor could it offer a framework for assessing more than an actor's capability.

Still other studies have been less explicit on how they treat the nature and role of intent in their frameworks and assessments. As noted above, the JCVI study on synthetic genomes covered a broad set of potential risks related to biosecurity and biosafety, including those related to bioterrorism, the risk to laboratory workers and to the public, and possible harm to the environment from accidental release. While the study notes that both state and non-state actors may have malicious intent to misuse synthetic genomics, its analysis is restricted to potential risks posed by non-state actors.

---

[78] Cummings CL, Kuzma J. Societal Risk Evaluation Scheme (SRES): scenario-based multi-criteria evaluation of synthetic biology applications. PloS one. 2017 Jan 4;12(1):e0168564., p. 8.

[79] Cummings CL, Kuzma J. Societal Risk Evaluation Scheme (SRES): scenario-based multi-criteria evaluation of synthetic biology applications. PloS one. 2017 Jan 4;12(1):e0168564., p. 8.

[80] Tucker, J.B. 2012. Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies. Cambridge: The MIT Press. p. 21. National Academy of Science, Engineering, and Medicine, *A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology* (Washington, DC: National Academies Press, 2017): p. 6.

[81] Tucker, J.B. 2012. Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies. Cambridge: The MIT Press, p. 72.

For most of the studies we have canvassed, there is an assumption that the intent of the actor is to cause as much harm as possible, usually to humans. Thus, actors engaging in misuse are assumed to be malicious or malevolent. There is a long-standing debate, however, on the extent to which non-state actors have the intent to acquire and use pathogens, toxins, and biotechnology to cause harm.[82] Furthermore, there is debate among experts about the objectives that malicious actors might have other than maximizing fatalities or injuries, e.g., causing mass disruption, demonstrating an advanced technology to emulate a nation-state, violating norms to demonstrate resolve, or satisfying some private grievance or psychological pathology. The Gryphon Scientific RBA is an exception to this observation since it discusses the motivations of a range of malicious, non-state actors.[83]

In summary, the biotechnology risk assessment literature focuses almost exclusively on how new technologies change the capabilities of non-state actors to cause harm. While the dominant type of misuse discussed is deliberate and malicious, most of the studies also addressed inadvertent and accidental harms that the technology could pose to laboratory workers, the public, or the environment. This literature mostly eschews any interest in or discussion of the motivations of non-state actors to misuse biotechnology or the factors that contribute to accidental or inadvertent releases of modified organisms. The one exception to this is the Gryphon Scientific RBA which explicitly addressed the causes of biosafety failures and trends in bioterrorism.

Benefit

Just as with the conceptions of risk described above, existing frameworks conceive of the benefits of biotechnologies in varying ways. The most common approach is to describe general potential benefits of biotechnology illustrated with prominent examples. The benefits of biotechnology are one of the fundamental assumptions of most of the preceding risk assessments discussed. For example, JCVI 2016 report conceives of the benefits of genome editing as contributing to the increased efficiency in research practices, production of vaccines for human and animal health, related human and animal diagnostics, new and improved drugs, carbon-neutral energy sources, bio-based manufacturing, and engineering specific pathways.[84] This should not be surprising since the benefits of biotechnology are often more self-evident than the risks they pose.

At the same time, it should be recognized that benefits and risks are inextricably linked, and ethical and social values also play a considerable role in how benefits and risks are defined. While the Tucker and 2017 NASEM frameworks explicitly exclude benefits from the scope of their studies, the degree of anticipated benefits has an implicit impact on how one analyzes the risks of the technology. Technologies with larger anticipated benefits across a wider range of applications will presumably be pursued more vigorously by researchers and companies, accelerating innovation, and diffusing knowledge, expertise, and technology more broadly and more quickly. Likewise, technologies with fewer anticipated benefits or more narrowly tailored applications will be developed more slowly by fewer actors. Since assumptions about the diffusion of expertise and

[82] Gregory D. Koblentz, "Predicting Peril or the Peril of Prediction? Assessing the Risk of CBRN Terrorism," *Terrorism and Political Violence*, Vol. 23, No. 4 (2011), pp. 501-520.
[83] Gryphon Scientific, Risk Benefit Analysis, pp. 862-868.
[84] Sarah R. Carter and Robert Friedman, J. Craig Venter Institute (JCVI), *Policy and Regulatory Issues for Gene Drives in Insects* (August 2016); Available at: http://www.jcvi.org/cms/fileadmin/site/research/projects/gene-drive-workshop/report-complete.pdf: pp. 10-12.

technology and rate of development are key factors in these risk assessment frameworks, the degree of expected benefits is an unstated antecedent condition for understanding the risks they pose.

Much of the literature fails to present governance approaches that address both the potential risks and the potential benefits of dual-use biotechnology. While some reports in the literature address the benefits of emerging technologies,[85] others either explicitly exclude benefits from their assessment[86] or acknowledge their existence without providing a framework for balancing the benefits and risks.[87] Overall, there seems to be consensus in the literature that there are indeed many benefits of biotechnologies, but many assessments largely focus on risks and security concerns.

Explicitly Excludes Benefits	Acknowledges Benefits	Explicitly Includes Benefits
NASEM, *A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology* (2017)	NRC, *Biotechnology Research in an Age of Terrorism* (2004)	NRC, *Globalization, Biosecurity, and the Future of the Life Sciences* (2006)
Cummings & Kuzma, *Society Risk Evaluation Scheme* (2017)	NASEM, *Gene Drives on the Horizon* (2016)	JCVI, *Synthetic Genomics: Governance Options* (2007)
	NSABB, *Oversight of GOF Research* (2016)	USG, *Companion Guide to Dual-Use Research* (2014)
	Tucker, *Innovation, Dual-Use, and Security* (2012)	Gryphon Scientific, *Risk Benefit Analysis (2016)*

Table 6. Technology Assessment Frameworks' Treatment of Benefits

The United States Government's 2014 *Companion Guide to Policies for Oversight of Life Sciences Dual Use Research of Concern* is one of the few attempts to explicitly include benefits in the assessment of dual use research.[88] While the steps outlined in the report do provide a method for assessing and weighing the potential benefits of emerging technologies, this checklist does not call for a determination of the magnitude of potential benefits or the feasibility and likelihood of realizing such potential benefits.

[85] Garfinkel MS, Endy D, Epstein GL, Friedman RM. "Synthetic genomics: options for governance," *Industrial Biotechnology*. 2007 Dec 1;3(4).; See United States Government (USG), *Tools for the Identification, Assessment, Management, and Responsible Communication of Dual Use Research of Concern: A Companion Guide*, Prepared by the National Institutes of Health (September 2014); Available at: http://www.phe.gov/s3/dualuse/Documents/durc-companion-guide.pdf: pp. 29-31.
[86] National Academy of Science, Engineering, and Medicine (NASEM), A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology (Washington, DC: National Academies Press, 2017): p. 5.
[87] National Academies of Science, Engineering, and Medicine (NASEM), *Gene Drives on Horizon*, (Washington, DC: The National Academies Press, 2016) doi: 10.17226/23405; Available at: https://www.gene-drives.com/gene-drives.pdf: p. 70.
[88] United States Government (USG), *Tools for the Identification, Assessment, Management, and Responsible Communication of Dual Use Research of Concern: A Companion Guide*, Prepared by the National Institutes of Health (September 2014); Available at: http://www.phe.gov/s3/dualuse/Documents/durc-companion-guide.pdf: pp. 29-31.

STEP 4: Assess the Potential Benefits
(a) Are there potential benefits to public health and/or safety from the research?
(b) Are there potential benefits of the research for agriculture, plants, animals, the environment, materiel, or national security?
(c) Will this research be useful to the scientific, public health, or public safety communities? If so, how?
(d) Because scientific research can have broad impacts, it is important to consider the scope of the potential benefits. Will the knowledge, information, or technology generated from the research be broadly applicable (e.g., to human health, multiple scientific fields, populations of organisms)? What populations of plants or animals might be positively affected?
(e) If a benefit has been identified, in what time frame (e.g., immediate, near future, years from now) might this research benefit science, public health, plants, animals, the environment, materiel, or national security?

Table 7. Steps for Assessing the Potential Benefits of Dual-Use Research of Concern

Balancing Benefits and Risk

There are few existing frameworks for balancing the benefits and risks of dual-use biological research. Tucker's framework applies a cost-benefit analysis approach, but provides little insight into how to characterize either costs or benefits of biotechnology or how political processes will weigh these when determining governance measures. Despite having commissioned a comprehensive, data-rich and methodologically sophisticated study on the risks and benefits of GOF research, the NSABB quickly recognized that "determinations about whether such studies should be undertaken involve value judgments based on weighing the risks and benefits."[89] This observation is not without precedent, as evidenced by the 1982 President's Commission for the Study of Ethical Problems in Medicine and Biomedical and Behavioral Research, which noted, "balancing present and future benefits and risks" was the key issue associated with genetic engineering in humans.[90]

The NSABB also commissioned an ethical analysis to elucidate the types of values that should be integrated into a decision-making framework. While this approach yielded a list of substantive and procedural values that should be considered in decisions to fund and publish gain of function research, the ethical review did not provide helpful guidance on how to apply these principles in

[89] National Science Advisory Board for Biosecurity (NSABB) 2016, Recommendations for the Evaluation and Oversight of Proposed Gain-of-Function Research, (National Institutes of Health: Office of Science Policy, 2016): p. 16.
[90] United States. President's Commission for the Study of Ethical Problems in Medicine and Biomedical and Behavioral Research. *Splicing Life: A Report on the Social and Ethical Issues of Genetic Engineering with Human Beings*. (Washington, DC: President's Commission for the Study of Ethical Problems in Medicine and Biomedical and Behavioral Research, 1982) Available at: https://bioethics.georgetown.edu/documents/pcemr/splicinglife.pdf.

practice.[91] One of the ethical values proposed for guiding GOF research was that of justice to ensure that the benefits and burdens of GOF were fairly shared and that the risks posed by this research did not disproportionately affect certain populations and that those who were exposed to these risks were not likely to benefit from the research.[92] The Gryphon RBA attempted to assess the degree to which GOF research, typically conducted in highly developed countries, complied with this value by evaluating the likelihood that developing countries would benefit from the improved vaccines, antivirals, and risk assessments that GOF research was expected to generate.[93] Despite this limited experience in operationalizing ethical values into assessments of the risks and benefits of dual-use research, these ethical considerations have been incorporated into the 2017 Office of Science and Technology Policy (OSTP) guidance on oversight of research with potential pandemic pathogens.[94] Whether ethical considerations provide a useful lens for weighing the risks and benefits of such research or add yet another complication to the process remains to be seen.

In its guidance to researchers on dual-use research of concern, the United States government offers a list of questions that principal investigators and institutional review committees should consider when weighing the risks and benefits of DURC (see Table 8).[95]

[91] National Science Advisory Board for Biosecurity (NSABB) 2016, Recommendations for the Evaluation and Oversight of Proposed Gain-of-Function Research, (National Institutes of Health: Office of Science Policy, 2016): p. 16.
[92] Michael J. Selgelid, *Gain-Of-Function Research: Ethical Analysis* (Melbourne, Australia: Centre for Human Bioethics, University of Monash, 2015), http://osp.od.nih.gov/wp-content/uploads/2013/06/Gain-of-Function_Research_Ethical_Analysis.pdf.
[93] Gryphon Scientific, Risk Benefit Analysis, pp. 433-455.
[94] Office of Science and Technology Policy, Recommended Policy Guidance for Departmental Development of Review Mechanisms for Potential Pandemic Pathogen Care and Oversight (P3CO), January 9, 2017, https://www.phe.gov/s3/dualuse/Documents/P3CO-FinalGuidanceStatement.pdf.
[95] United States Government (USG), *Tools for the Identification, Assessment, Management, and Responsible Communication of Dual Use Research of Concern: A Companion Guide*, Prepared by the National Institutes of Health (September 2014); Available at: http://www.phe.gov/s3/dualuse/Documents/durc-companion-guide.pdf: pp. 29-31.

STEP 5: Weigh the Risks and Benefits
(a) Could the information of concern be more readily applied to improvements in surveillance or to the development of countermeasures than to malevolent applications? What reasons or evidence support the answer to this question?
(b) What is the time frame in which potential benefits might be realized?
(c) How might the potential benefits and the anticipated risks be distributed across different populations (humans and animals)? Who or what will be the likely beneficiaries of the potential benefits? Will the potential benefits be distributed equally or disproportionately across different populations? Here, it will be helpful to keep in mind that, for example, human populations may differ in terms of size. The potential benefits may accrue to a large or, alternatively, to a small number of individuals. Or, human populations may differ along socioeconomic or cultural lines. The potential benefits may accrue to or have little impact on a vulnerable or low-resourced population versus a well-resourced population. Who or what will bear the anticipated risks? Is it likely that one or more specific populations will bear the burden of anticipated risks?
(d) Considering the anticipated risk in tandem with the potential benefits, are the risks of such a feasibility and magnitude that they warrant proceeding after developing and implementing a risk mitigation plan? Are the potential benefits of significant magnitude to warrant proceeding despite the risks? What is the more responsible way to proceed? For the vast majority of cases of DURC, an appropriate risk mitigation plan can be developed and effectively implemented.

Table 8. USG Recommended Steps for Weighing Risks and Benefits of Dual-Use Research of Concern

As the USG notes, balancing and weighing the benefits and risks of emerging technologies "is the most challenging step in the risk-benefit assessment...This language, however, suggests that risks and benefits can be quantified and that they are commensurable. This is rarely, if ever, the case."[96] The assessments of both the benefits and risks will likely be qualitative and fraught with uncertainty in terms of likelihood, consequences, time frame, and population most likely to be impacted.

The H5N1 controversy highlighted the widely divergent views on the benefits and risks of dual-use research held by different stakeholders, including, scientists, publishers, biosecurity experts, the national security community, and public health officials. Dual-use research features many of the same attributes as wicked problems which are "characterized by multiple, overlapping subsets of problems and high levels of social complexity driven by the diversity of players involved in problem-solving."[97] There is also evidence of similar divergence among stakeholders in the debate over genome editing in general and gene drives in particular:

[96] United States Government (USG), *Tools for the Identification, Assessment, Management, and Responsible Communication of Dual Use Research of Concern: A Companion Guide*, Prepared by the National Institutes of Health (September 2014); Available at: http://www.phe.gov/s3/dualuse/Documents/durc-companion-guide.pdf: p. 30.

[97] Gregory Koblentz. 2014. "Dual-use research as a wicked problem," *Frontiers in Public Health*, 2(113); Available at: https://www.frontiersin.org/articles/10.3389/fpubh.2014.00113/full: p. 1.

> The values attached to the potential environmental outcomes may be understood in different ways, some of which are not universally accepted. As a result, how they are to be weighed against each other and alongside public health and agricultural outcomes is very complicated.[98]

Although the Cummings and Kuzma article focuses on psychological and social factors that influence the perception of risk, similar mechanisms likely impact the perceptions of benefits as well. Thus, policy-makers must be sensitive to not only the quantitative and qualitative aspects of risk-benefit analyses but also broader societal factors that may influence the acceptability of certain risks and the values placed on certain benefits.

To compensate for the variability of conceptions of risks and benefits based on different social and cultural values, the USG guidance recommends that the balancing of risks and benefits be managed by a broad selection of individuals with diverse backgrounds, experience, and perspectives:

> Discussion and debate within such a group can help to (a) identify and mitigate the biases that individuals inevitably bring to the challenges of this sort, (b) uncover often implicit assumptions in arguments, (c) scrutinize and test the basis for judgments, and (d) yield conclusions that represent a consensus (literally, "a thinking together") and are optimally defensible.[99]

The shift from relying considerably on expert judgment, often to the exclusion of affected publics, to a more inclusive approach that includes democratic engagement is a welcome one.[100]

---

[98] U.S. National Academies of Science, *Gene Drive Research in Non-Human Organisms: Recommendations for Responsible Conduct* (Washington, DC: U.S. National Academies of Science, 2016), http://www.nap.edu/catalog/23405/gene-drives-on-the-horizon-advancing-science-navigating-uncertainty-and. p. 70.

[99] United States Government, *Tools for the Identification, Assessment, Management, and Responsible Communication of Dual Use Research of Concern: A Companion Guide*, Prepared by the National Institutes of Health (September 2014); Available at: http://www.phe.gov/s3/dualuse/Documents/durc-companion-guide.pdf: p. 30.

[100] This shift can be seen in comparing the approach by the 1982 President's Commission for the Study of Ethical Issues in Medicine and Biomedical and Behavioral Life Sciences and the 2010 Presidential Commission for the Study of Bioethical Issues. The former advocated for a heavy reliance on expert judgment, while the latter called for widening the aperture of who benefits and who makes decisions regarding technology to include public participation and democratic deliberation. United States. President's Commission for the Study of Ethical Problems in Medicine and Biomedical and Behavioral Research. *Splicing Life: A Report on the Social and Ethical Issues of Genetic Engineering with Human Beings*. (Washington, DC: President's Commission for the Study of Ethical Problems in Medicine and Biomedical and Behavioral Research, 1982) Available at: https://bioethics.georgetown.edu/documents/pcemr/splicinglife.pdf.

Our Preliminary Approach to Assessing the Risks, Benefits, and Governability of Dual-Use Biotechnologies

To ensure a thorough consideration of the security implications of genome editing, as an initial guide the project team is adapting and extending a technology assessment framework developed by Jonathan B. Tucker.[101] The current adaptation of this framework is composed of three parts: an assessment of the risk of the technology being misused (intentionally and/or accidentally), the benefits of the technology, and an assessment of the technology's governability. This framework, in addition to the guiding questions contained in the project briefing memo, provides criteria against which the project team and issue brief authors can compare and organize their analyses both in the issue briefs and in the two workshops. A common frame of reference is intended to facilitate a comprehensive assessment of the risks, benefits, and governance landscape of genome editing technologies, and a comparison across different applications, domains, and industries. At the same time, the criteria listed below, as with the issue brief topics and questions, are illustrative and not definitive. Study participants are welcome to suggest their own frameworks and criteria and/or devise alternative ways of measuring the criteria listed. This framework provides an initial basis from which to select from a menu of options for governing the technology. Our intention is to leverage the project's process to evaluate the assumptions embedded within the existing biotechnology risk assessment, governance, and policy frameworks. We intend to examine the viability of different governance options for genome editing moving forward and the implications for policy and practice. These options range from hard law, such as legislation and regulation, to soft law, such as voluntary guidelines and self-governance measures to informal measures, such as codes of conduct. These options in turn may be pursued by different sets of stakeholders. This study has chosen to examine the risks and benefits of genome editing in the near term (less than five years) and the medium term (5-10 years).

Risk Assessment

Potential criteria to assess the risk of a technology include:

Range of Malicious Applications: How many different types of malicious applications does the technology have? Is the technology highly specialized and applicable to only a small number or narrow range of applications or is it highly versatile with a wide range of potential applications? Does the technology present unique risks that are not otherwise present?

Magnitude of Potential Harm: What is the scale of potential consequences of misuse measured in deaths and injuries, direct and indirect economic costs, and social impact? What is the distribution of vulnerabilities to such consequences? How difficult and expensive is it to reduce these vulnerabilities? What is the distribution of existing countermeasures to such consequences?

[101] Jonathan B. Tucker, ed., Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies (Cambridge: MIT Press, 2012).

If there are shortfalls or gaps in countermeasures, how difficult and expensive would it be to remedy these weaknesses? What is the net assessment of the potential consequences given the distribution of vulnerabilities and countermeasures?

Imminence of Potential Misuse: Given the current maturity of the technology and its anticipated future trajectory, how soon would a state or terrorist group be able to use this technology for malicious purposes? What is the risk of accidents as compared to intentional misuse?

Benefit Assessment

Potential criteria to assess the benefits of a technology:

Range of Beneficial Applications: How many different types of beneficial applications does the technology have? Is the technology highly specialized and applicable to only a small number or narrow range of applications or is it highly versatile with a wide range of potential applications?

Magnitude of Potential Benefits: What is the expected magnitude of the benefits provided by the technology as measured by the number of lives saved or improved, direct economic benefits, and indirect economic benefits such as increased productivity? Will the technology provide unique benefits that would not otherwise be available? How large is the population expected to be of the primary beneficiaries of the technology's applications? Will the benefits of the technology have broad and diffuse effects or be captured primarily by a narrow or small population?

Imminence of Potential Benefits: Given the current maturity of the technology and its anticipated future trajectory, how soon will the benefits of the technology be realized? How reliant are the benefits of the technology on other technologies and how mature are those technologies? How high are the national legal, policy, and/or regulatory hurdles that would need to be overcome to realize these benefits? To what extent is international agreement or cooperation needed to realize these benefits?

Assessment of Governability

Potential criteria to assess the amenability of a technology to different governance approaches:

Accessibility: How easy is it to acquire the necessary hardware, software, and information? Is the technology and information commercially available, proprietary, under patent protection, or restricted due to classification? How expensive is the technology? How dependent is the technology on other upstream or downstream technologies?

Expertise: What type and level of expertise is needed to use the technology? How common is this type and level of expertise? How much of the required expertise depends on tacit knowledge? How available is this tacit knowledge and how easily transferred is it? Are there indicators that the level of expertise required to use the technology is decreasing, i.e., deskilling?

Embodiment: To what degree is the technology embodied in specialized hardware that is easily controlled or intangible information that is easily shared? To what extent is similar hardware or information already subject to national or international governance?

Maturity: Where does the technology lie on the development pipeline ranging from basic research to applied research to advanced development to commercialization?

Convergence: To what degree is the technology the result of a convergence between multiple scientific disciplines?

Rate of Advance: How quickly is the technology advancing in terms of reliability, speed, throughput, accuracy, or cost? Is the rate of advance linear, exponential, incremental, or declining?

Diversity and Influence of Key Stakeholders: Do key stakeholders share the same values and interests and have comparable levels of political influence or do stakeholders hold diverse values, have asymmetries of interest, and unequal levels of political influence?

Degree of International Diffusion: How many international sources of the technology are there? How easy is it to transfer the technology across national borders?