Bulletin of the Atomic Scientists

Biotech promises miracles. But the risks call for more oversight

By David Gillum, George Poste, Craig Woods, Rachel Levinson | August 31, 2023

The "gene machine" was an early DNA synthesis machine produced in the 1980s. Progress in biotechnology, including significant advances in gene synthesis capabilities, heralds many advances, but may also require new systems of oversight to guard against biosecurity risks. Credit: National Museum of American History.

Some inventions, Abraham Lincoln once said, are of "peculiar value, on account of their great efficiency in facilitating all other inventions and discoveries." Although many examples of disruptive ingenuity predate Lincoln's 1860 speech, the list has grown rapidly since—and with revolutions seemingly occurring at a greater frequency. Consider electricity, aviation, antibiotics, vaccines, nuclear energy, space travel, the internet, and most recently, generative artificial intelligence. Like other

groundbreaking innovations, many of these technologies can be put toward peaceful or malevolent ends, depending on the goals of who is using them.

Now it's the rise of biotechnology, a sector with its origins in the ability to sequence, synthesize, and edit the genes of organisms, that is joining the pantheon of advances that pose perplexing dual-use implications. Life sciences progress is creating both the potential for unprecedented benefits in medicine (and other areas) as well as new risks of harm from accidents, unforeseen consequences, or even deliberate abuse. There has never been a major technological disruption that countries haven't sought to use for industrial or military superiority, or for terrorists and criminals in pursuit of their aims. The examples of historical bioweapons programs and bioterrorism suggest that these maxims will likely remain the case as the bioeconomy grows.

Despite the dramatic pace of discoveries in the life sciences, however, the regulatory systems established for other dual-use risk domains, such as chemical and nuclear research, remain far more mature than those for oversight of the bioeconomy. This reflects fears stemming from the last century's wars—the chemical trench warfare of World War I and nuclear bombings during World War II—as well as from the health and environmental consequences of accidents in the nuclear and industrial sectors like Chernobyl or the Deepwater Horizon oil well disaster.

The oversight of scientific research exists at international, national, state, and institutional levels and within multiple agencies and jurisdictions. Regulations, guidelines, and policies on the safety and security of scientific research have been ratified in many legal instruments. The outdated mode of biosecurity governance starts at the level of global diplomacy.

The 1972 Biological Weapons Convention, now signed by 183 nations, was designed to prohibit the development, production, acquisition, transfer, and stockpiling of biological and toxin weapons. The type of hazards identified in the convention have not kept pace with advances in molecular biology, genetics, and synthetic biology. And within the United States and elsewhere, these powerful technologies, now increasingly combined with progress in engineering, autonomous robotics systems, and advanced computing, substantially complicate the development of all embracing regulatory and legislative oversight frameworks that look beyond simply controlling pathogen research to limit risks without constraining growth in the global bioeconomy.

Developing a well-balanced oversight system will not be easy. Nonetheless, the expanding gaps in national and international governance of dual-use biotechnology dictate that this subject be a core component of national security policies.

The evolution of biological dual-use risk oversight. Building on experiments in the 1950s that established DNA as the genetic code of life, the science of manipulating genomes, modifying genetic control mechanisms, and creating novel biological functions and organisms not seen in nature progressed rapidly. But with these advances came increasing public concern over progress in genetic research.

Paul Berg, a biochemist, played a role in precipitating the controversy over recombinant (hybrid) DNA with his work in the 1970s introducing bacterial genes into a virus known to cause tumors in rodents. Although Berg had planned to introduce the modified viral DNA to bacterial cells, concern over whether infected cells could escape and cause human cancers ultimately led him to pause the work. Berg and other scientists organized the Asilomar Conference on recombinant DNA in 1975 with the goal of assuaging public fears over the new technology and touting the capability of the scientific community to self-police. The now-famous conference led to guidelines for government-sponsored genetic engineering research, but no onerous new rules—arguably a light-touch oversight approach in the life sciences that has largely endured.

In the almost 50 years since Asilomar, oversight of dual-use biotechnology in the United States has mainly focused on the original fears surrounding the Berg experiment: the risks associated with the manipulation of pathogens. This is likely in part a legacy of Cold War-era concerns about covert development of biowarfare agents—including by nations who signed on to the Biological Weapons Convention. What biosecurity policy still lacks is a holistic approach to regulation of the biotechnology-driven modifications of humans, animals, plants, and microorganisms.

With the rise of several radical and terrorist groups over the last few decades, the prospect of bioterrorism by substate actors has heightened concerns over the misuse of pathogens. The 2001 anthrax attacks, for example, galvanized the US government and others to implement controls on the use and distribution of the microbial agents deemed most likely to be deployed by adversaries, the so-called “select agents.”

In the same era, academic research demonstrating how science could be used to design and assemble synthetic viruses prompted the formation of the National Science Advisory Board for Biosecurity in 2005 to evaluate dual-use risk from federally funded biotechnology research, conducted primarily in academia. The board’s formation represented a departure from policy geared toward stemming bioweapons or bioterrorism and the US government’s focus remained clearly on pathogens.

After research groups published studies on making highly pathogenic avian influenza airborne transmissible among mammals, the National Institutes of Health expanded their focus to consider biosecurity risks. The NIH’s oversight actions in 2014 and 2017 took aim at “gain-of-function” experiments, such as those that could induce specific

mutations or modifications to enhance a pathogen's virulence, transmission, or immune evasiveness. The COVID pandemic only intensified public and legislative concerns about pandemic diseases and the risk-benefit calculus involved in gain-of-function research. New recommendations in 2023 from the biosecurity advisory board sought to further tighten oversight of pathogen research and to increase biosafety measures against accidental release.

Looming gaps. While attention on pathogen research is clearly warranted, to better anticipate future risks originating from the life sciences research and the bioeconomy, regulators and the scientific community must now expand the horizon for dual-use research beyond a narrow focus on select agent pathogens. Trying to predict which pathogen will cause future harm, and whether it is existing or modified in nature or artificially created, is a continuous challenge. In addition, there are recent innovations in biotechnology that are raising biosecurity concerns: Artificial Intelligence (AI) could be used to develop blueprints for novel pathogens; experiments conducted using software and complex algorithms could predict the makeup of organisms that are more infectious and transmissible to humans, plants and animals; benchtop devices may eventually be used to synthesize nucleic acids to aid in the creation of pathogens; and personal genetic screening databases could potentially allow for the creation of targeted bioweapons. Broadening the aperture of what biosecurity oversight should encompass will be complex.

The National Science Advisory Board's policies on pathogenic organisms—which have so far been embraced by the US government—apply to federally sponsored research, most of which occurs in academia. But they do not address private sector research. As the advisory board's latest set of recommendations points out, increased federal, state, and local government oversight of the private sector would help to create "a national culture of responsibility."

But even if existing biosafety and biosecurity regulations were expanded to include the private sector, which government agencies would have lead responsibilities for oversight of different types of biorisk remains ill-defined. Similarly, without international harmonization of dual-use guidelines, the prognosis for orderly and responsible global development of these technologies will remain problematic.

The unifying principle in biotechnology research is understanding the varied genetic regulatory networks and molecular circuitry that encode biological functions in different life forms, from single-cellular microorganisms to humans. This knowledge provides the foundation for ever more precise manipulation of biological systems. The evolution of precision medicine, precision agriculture, environmental bioremediation, and novel industrial bioprocesses illustrates the myriad positive benefits of

biotechnology—but the same insights into the organization of the molecular systems creates almost limitless vulnerabilities for their deliberate, targeted disruption.

Technological convergence. Dual-use life sciences progress isn't occurring in a vacuum.

A new oversight framework must address the implications of the confluence of the life sciences with engineering and large-scale computing platforms. The potential applications of using AI to expand the spectrum of chemical and biological weapons has attracted high-level attention in the United States and overseas. AI has already been used to simulate chemicals with increased toxicity and to design algorithms for pharmaceuticals that could also be used as biochemical weapons to disrupt diverse bodily functions. There are growing concerns that new AI platforms could develop proteins or synthetic biological constructs—and that could serve to make the process of developing biological weapons easier, by helping to lower barriers to access, like advanced scientific knowledge.

Conversations about how to control AI have been going on for years. Yet, it is only now triggering a tsunami of panicked legislative hearings and media think-pieces. Even so, the daunting task of assessing the dual-use risk implications of AI and emerging biotechnologies has not yet reached the necessary level of conversation with a broader audience. Could ChatGPT and desktop gene synthesis machines be used to create the next pandemic pathogen or design ethnic specific bioweapons? Theoretically, yes (as described in a recent publication from MIT). A more pragmatic critique, however, is necessary to evaluate the technical barriers, skill gaps, and logistics implicit in making such hypothetical threats a reality.

Open access. Amid the dual-use risks posed by new biotechnology, there is another component that is lacking in, at least, US biosecurity governance: clear policies for dealing with information hazards.

Earlier efforts to engage leading scientific journals to adopt editorial policies to identify open research source data that could be usurped for malicious intent have been largely unsuccessful. This was largely based on reflexive opposition from the academic research community as eroding the fundamental tenet of academic freedom, as well as the US National Security Directive 189, which calls for, "to the maximum extent possible, the products of fundamental research remain unrestricted." Examples, however, abound about the potential risks of placing biotechnology information in the open literature.

The federal government also has a moral imperative to develop and disseminate training and educational curriculum for life sciences researchers. Increasing the exposure that undergraduates and graduates in the life sciences get to biosecurity concerns would be a welcome reform. To encourage greater biosafety and biosecurity awareness, such training materials could be made into a requirement for receiving federal funds

A path forward. Biotechnology is changing so quickly that rules adopted today are unlikely to match the speed and scale of life science innovation. In a narrow sense, regulators must provide clear guidance on how and when to report research with the potential to cause major harm and define accountabilities for failing to do so. More broadly, a renewed social and cultural awakening among life science communities on the scope of dual-use technologies in biological and medical research is long overdue.

Implementing a new oversight system will require: forming new coalitions of expertise drawn from government, academia, and industry; improving the coordination of biosecurity policies across government agencies both within countries and internationally; and the creation of systems and tools to identify, mitigate, and attribute misuse. US biosecurity policy focused on pathogen misuse for decades and failed to take into account the broader capabilities of biotechnology. At the same time, it has largely been focused on publicly-funded research while ignoring the role private resources play in advancing biotechnology. What is necessary is policymaking that is agile and that can adapt to the expansion of new dual-use technologies.

Meaningful progress in domestic and global biotechnology governance may represent one of the grand challenges of the coming decade in shaping security policies while ensuring peace and commercial innovation.