EMILY MULLIN SCIENCE NOV 1, 2022 8:00 AM

How to Detect a Man-Made Biothreat

The US government is funding tech to determine whether genetic alterations in a virus or pest are an evolutionary quirk—or a lab-engineered danger.

Draper is developing a chip capable of identifying genetically engineered organisms in soil, water, and other samples. COURTESY OF DRAPER LABORATORY OF BOSTON

A NEW, HIGHLY transmissible strain of influenza emerges. A pesticide-resistant insect decimates huge swaths of crops. A patient winds up in the emergency room with a bacterial strain that doesn't respond to any available antibiotics. Any of these scenarios could happen due to natural evolutionary changes among pathogens or pests. But as genetic engineering gets cheaper and easier, it's becoming increasingly plausible that they might one day be the product of deliberate manipulation.

To guard against these potential threats, the US government is funding the development of tests to detect dangerous bioengineered organisms before they have a chance to cause significant harm. The effort was announced in 2017 by the Intelligence Advanced Research Projects Activity, or Iarpa, within the Office of the Director of National Intelligence. In a livestreamed update in October, Iarpa program manager David Markowitz announced that two platforms developed under the program were both 70 percent accurate at identifying the presence of bioengineering. "We simply never know what sample is going to come through the door in a government lab, and we need to be prepared for anything," Markowitz said during the news briefing.

One of the platforms, created by the nonprofit Draper, based in Cambridge, Massachusetts, is a rapid, handheld testing device that uses a thumbnail-sized chip to detect engineered genetic material. The other is software developed by Boston biotech company Ginkgo Bioworks that uses machine learning to identify engineering in genomic data generated from sample organisms. (The companies haven't yet published their results in a peer-reviewed journal, and their platforms are still in development.)

Crops and animal feed are already widely screened to determine the presence of genetic traits that can't be found in nature or created through conventional breeding. Scientists use a test called PCR, or polymerase chain reaction, to identify whether bioengineered DNA is present and in what amount. When it comes to food labeling, scientists usually know what genetic change they're looking for. But no general-purpose tool exists for detecting engineered genetic material in bacteria, viruses, or other organisms that could appear in any context.

Until now, detecting the presence of bioengineering relied on manual analysis, which is labor-intensive and slow. Through a process called sequencing, researchers can generate a readout of an organism's entire genetic code: a series of As, Cs, Gs, and Ts, or bases, which make up the building blocks of life. Every microbe, plant, animal, and human has a unique configuration of these letters.

To determine whether an organism's genetic code has been tinkered with, scientists need to know what its genome—and those of its close relatives—normally look like. Then they can search for areas that look out of the ordinary.

DNA can be manipulated through at least a half dozen processes. A conventional method involves adding a gene from one species to another—usually for bioengineering crops. Chunks of DNA can also be moved from one part of an organism's genome to another part, a type of change called a translocation. Crispr gene editing, which is being explored as a way to treat diseases in people, and to improve plants and animals bred for human consumption, can delete chunks of DNA. Older editing techniques, such as zinc finger nucleases and Talens, have also been used for these purposes but haven't been as successful as Crispr.

Any of these processes may leave behind signatures of bioengineering. For example, scientists can tell if a gene has been added or moved by comparing that organism's genome to a reference sample. When using Crispr, deletions sometimes turn up in other parts of the genome that look like the targeted section, but aren't. Talens and zinc finger nucleases also have a tendency to produce these "off-target" effects. The deliberate use of radiation can also produce traceable DNA mutations.

Draper and Ginkgo's technologies are designed to detect these common signatures of engineering. Ginkgo's software also relies on algorithms that compare the genome being analyzed against those in a huge database to determine whether it looks like an engineered or natural one. Draper's device is meant to be deployed quickly in the field on single samples, while Ginkgo's is designed to do large-scale analysis of many samples.

"Genetic engineering has been happening for quite a while now, and it's become

increasingly easy to do it," said Laura Seaman, principal scientist at Draper, during the livestream. "It's important to understand how these tools are being used and to identify them in an unknown situation."

When Iarpa launched the Felix program (short for Finding Engineering-Linked Indicators) that produced these efforts, the agency had set the ambitious goal of developing technologies that would be 90 percent effective at detecting the presence of engineering. In that regard, the Iarpa awardees have some improving to do.

In a test Iarpa ran this spring and announced October 17, government scientists evaluated the technology on 100 samples of both engineered and natural organisms taken from a variety of places, including soil, mouse feces, and a cow's stomach. Among these were 73 samples of bioengineered organisms, many of which were mixed with other organisms that weren't engineered. "We tried to make these batches representative of the real-world challenges that the biosecurity community faces every day," Markowitz says.

According to Markowitz, the Draper and Ginkgo teams correctly identified 70 percent as being bioengineered. Draper had no false positives, while Ginkgo had one—results stating that bioengineering was detected when it was actually not present. A bigger problem for both teams was the rate of false negatives, or failing to identify bioengineering when it was in fact present. For one thing, the platforms didn't perform well on samples that contained very subtle genetic modifications, such as a single A or T that got swapped. These types of modifications can be made with a relatively new technique called base editing, which makes single base-letter changes instead of cutting whole genes or chunks of genes, like classic Crispr editing does.

The platforms also had a harder time detecting evidence of engineering in samples from organisms with large genomes, according to Markowitz. "The larger the genome of the organism is, the more training data you need to get a statistical model, and the more you have to sift through in order to find the signatures of engineering," Markowitz says.

Making the technology more accurate will require a bigger, more diverse dataset—more reference genomes of the organisms all around us. “We should be sequencing everything that is around us and monitoring what is there,” says Joshua Dunn, head of design at Ginkgo. “It will help us understand the baseline of what is normal, so that if we see any deviation from that we can zero in on the parts of the sample that are the most interesting.”

(Iarpa did not release performance data for technologies developed by the program’s four other participants: The Broad Institute of MIT and Harvard, Harvard University’s Wyss Institute, Noblis, and Raytheon.)

But even if the platforms’ accuracy improves, it’s hard to know whether they would be able to detect a completely new organism that scientists have never seen before. Richard Ebright, a molecular biologist at Rutgers University, is skeptical that any technology will be able to definitively identify a bioengineered organism. “There is no technology—none—that comprehensively and reliably can distinguish between an engineered genome sequence and a natural genome sequence, and there never will be,” he says. “There are too many ways to manipulate a genome without leaving signatures of manipulation.”

This includes a technique developed more than a decade ago called seamless ligation of nucleic acids, or Slice, which uses bacterial enzymes to join DNA fragments. Older methods, such as selective breeding or serial passage —repeatedly growing viruses or bacteria in new environments over time—also would be unlikely to leave signatures of engineering, he says.

And Gigi Gronvall, a senior scholar at the Johns Hopkins Bloomberg School of Public Health who focuses on biosecurity, says the genetic sequence of a new pathogen isn’t the only factor to consider when determining whether a biothreat has been engineered. “If there was suspicion of deliberate misuse, attributing that to a particular actor is going to rest on lots of pieces of evidence,” she says. Factors such as where a new pathogen emerges, who it initially infects, and how it spreads, need to be considered. “Being able to identify these signatures that indicate bioengineering is important, and I hope we continue to get better at it. But it’s never going to be 100 percent of the picture,” she says.

Not all engineered organisms are dangerous, of course. Companies are engineering bacteria, viruses, plants, animals, and human cells with benefits that might help treat diseases or create new foods. Markowitz says bioengineering detection could help these companies protect their intellectual property.

But governments will likely be the main users of the technology. Markowitz says Iarpa has already made the platforms available to other US government agencies. ("I can't speak to how these tools are being used currently, but I will say that for several months they have been in the hands of a very large number of both domestic and international partners," he says.)

And he confirmed that early on in the Covid-19 pandemic, Iarpa used technology from the Felix program to determine that the SARS-CoV-2 virus was not bioengineered. The idea that SARS-CoV-2 was engineered in a lab has since been thoroughly discredited, but at the time some scientists had questioned whether a part of the virus called the furin cleavage site, which is responsible for its high infectivity, was evidence of engineering, because some of the virus's closest relatives don't have this feature.

Gronvall says the theory flourished in part because of scientists' limited knowledge of coronaviruses. It turns out other coronaviruses have these sites as well. "It only seemed suspicious until we looked at more of the coronavirus family and realized that our *n* was just really low. We were only sampling a very tiny portion of what was out there," she says. "Now that our field of knowledge is greater, it's not so unusual anymore."

Ultimately, these testing platforms might not only detect future engineered biothreats, but help deter labs from creating them in the first place. "Any would-be bad actor, just by virtue of knowing that the tools to rapidly detect what they're trying to do are out there, might think twice," Markowitz says.

More Great WIRED Stories

- 📩 The latest on tech, science, and more: Get our newsletters!
- The hunt for the dark web's biggest kingpin
- How to extract text from any image
- The world is drowning in plastic
- America's Adderall shortage could kill people
- The quiet insurrection the January 6 committee missed
- 👁 Explore AI like never before with our new database
- ✨ Optimize your home life with our Gear team's best picks, from robot vacuums to affordable mattresses to smart speakers

Emily Mullin is a staff writer at WIRED, covering biotechnology. Previously, she was an MIT Knight Science Journalism project fellow and a staff writer covering biotechnology at Medium's OneZero. Before that, she served as an associate editor at MIT Technology Review, where she wrote about biomedicine. Her stories have also... Read more

STAFF WRITER

TOPICS BIOTECH BIOLOGY GENETICS GENETIC ENGINEERING DNA CRISPR DISEASES AGRICULTURE GOVERNMENT