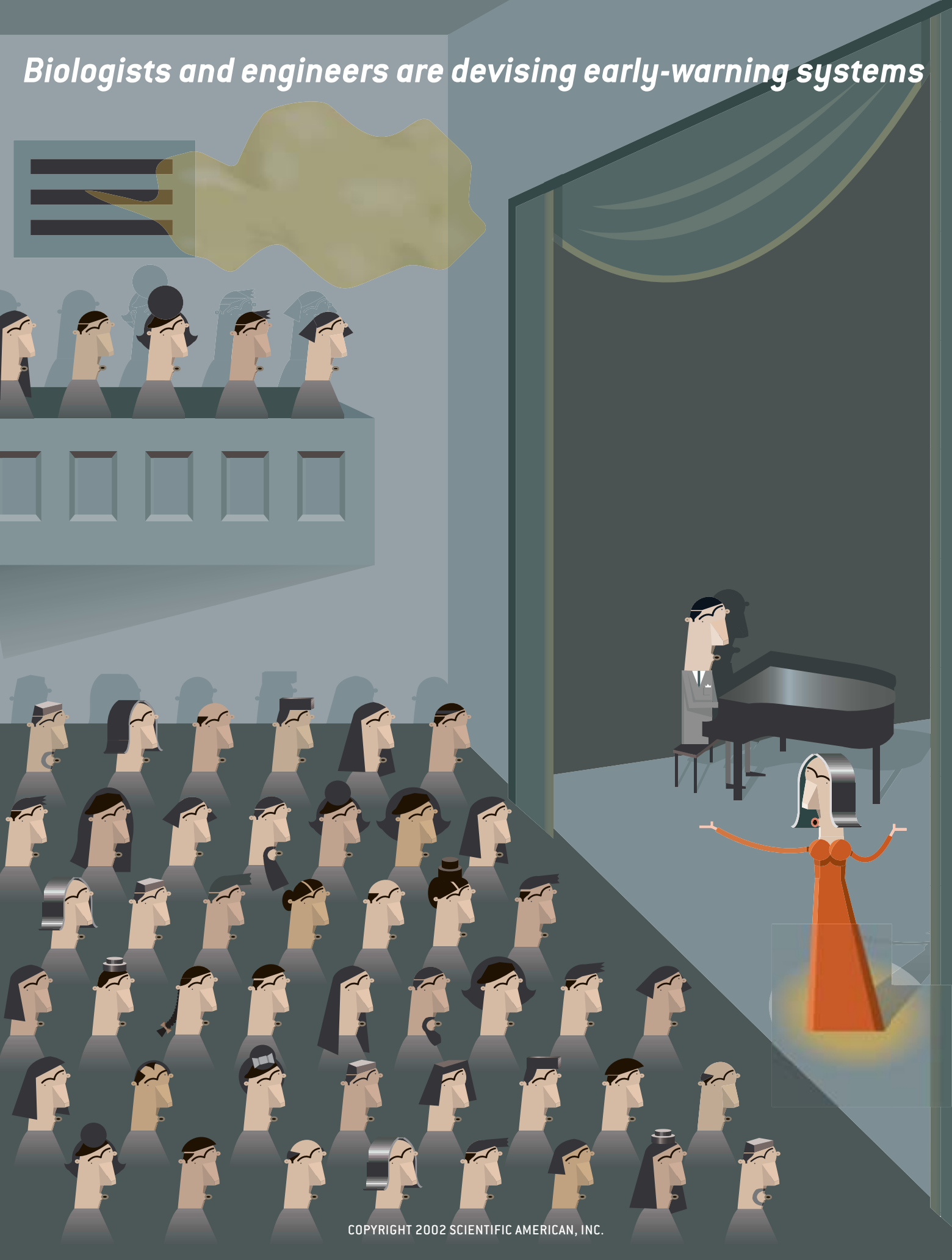
Biologists and engineers are devising early-warning systems



COPYRIGHT 2002 SCIENTIFIC AMERICAN, INC.

that can detect a bioterrorist attack in time to blunt its effects

TECHNOLOGY AGAINST Terror

By Rocco Casagrande

In May 2000 high-ranking members of the U.S. government watched as a cloud of bacteria wafted through the Denver Center for the Performing Arts, a complex of seven theaters that seats a total of 7,000. One week later thousands of people were dead or dying from the plague, the state borders of Colorado were closed, food and medical supplies began to run short, and medical care was all but shut down as doctors and nurses fell ill and antibiotics were used up. Luckily, this scenario wasn't real; it was a computerized exercise to simulate the effects of a biological attack against a target in the U.S. Part of a test named TopOff, it served as a wake-up call to civic leaders that they can't wait for sick people to start showing up at emergency rooms if they hope to wage an effective defense against biological weapons. Scientists are now devising a range of early-warning systems to alert government officials to an attack as it is happening. These technologies include DNA- and antibody-based biochips as well as "electronic noses" that can sniff out deadly microbes.

Are We Under Attack?

BIOLOGICAL WARFARE is insidious. Airborne clouds of bacterial or viral agents are nearly invisible and odorless; people who inhale the agents would not know they had been attacked until they fell ill days later. By that time, it might be too late to treat those victims or to protect others from infection. Although most biological agents are not very contagious, in many instances the unknowingly infected could pass on the disease.

Fortunately, the incubation period of biological agents provides a window of time in which public health officials could quarantine and treat victims and vaccinate others. Prior to the onset of symptoms, many diseases caused by biological agents are treatable with antibiotics; after symptoms appear, some victims will be beyond treatment.

Early detection is particularly important because many of the diseases caused by biological warfare agents trigger initial symptoms, such as fever and nausea, that could easily be mistaken for the flu. Medical students are generally taught the phrase "When you hear hoofbeats, think horses—not zebras," as a way to remind them to rule out common disorders before considering more exotic diagnoses. Although this dictum saves time and effort in everyday situations, it could lead doctors to initially overlook a biological attack. For this reason, some biological detectors are colloquially referred to as zebra chips, or Z chips, because they can tip off physicians that a metaphorical zebra is on the loose.

Biological warfare can be waged by contaminating food or water supplies or via disease-carrying insects such as mosquitoes, but these methods are unlikely to affect thousands of vic-

FRED RIX

COPYRIGHT 2002 SCIENTIFIC AMERICAN, INC.

tims during a single attack. Biological weapons reach the level of weapons of mass destruction—with a potential for human casualties rivaling that of nuclear weapons—only when they are disseminated through the air as a breathable aerosol of particles about one millionth of a meter in size. These tiny droplets can float through the air for long distances and become lodged deep within the lungs to cause dangerous systemic infections.

Airborne biological agents are tough to detect, however, because of their variety: they can come in the form of bacteria, viruses or nonliving toxins produced by microbes. Biological agents can be deadly, even when extremely dilute. A healthy person breathes in roughly six liters of air a minute, and certain pathogens can cause disease when as few as 10 organisms are inhaled. To protect people who are present for short periods in a contaminated area, a device would have to pick up two individual pathogens per liter of air—an extremely daunting task.

The first successful biological detectors merely spotted clouds of small particles. Some of these machines—such as the U.S. Army's XM2, which was deployed during the Gulf War—sample the air around them and are linked to machines that count particles of the appropriate size for bioweapons. If that particle count exceeds a certain threshold, an alarm sounds to notify troops to evacuate the area. Other particle detectors employ lidar, a system much like radar that emits a laser beam and then detects the light that bounces back from objects in its path. In dry conditions, lidar-based devices function from a distance of 50 kilometers, but they cannot distinguish between mists of biological agents and clouds of fine dust or smoke.

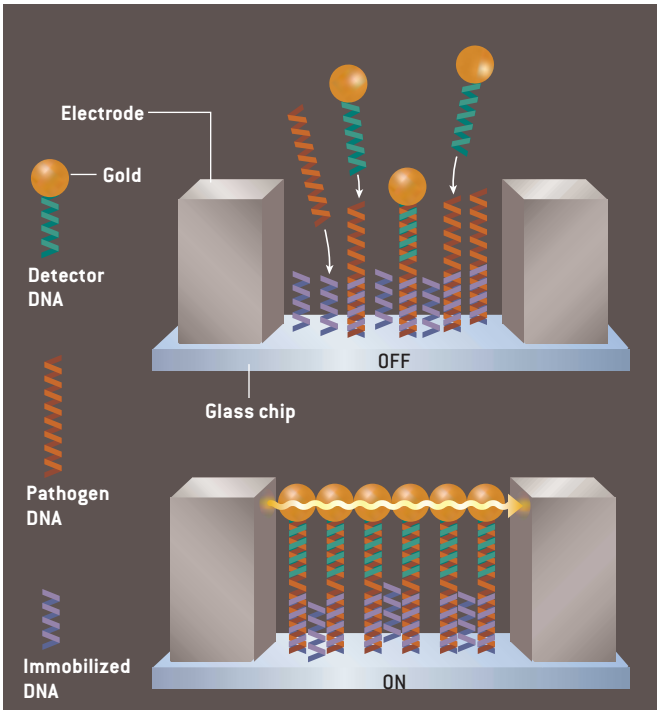
Newer lidar systems take advantage of certain molecules in almost all living cells that fluoresce when excited by ultraviolet (UV) light. These UV-lidar devices excite particles with a UV beam and watch for fluorescence emitted from the cloud. But even UV-lidar cannot discern pathogens from clouds of harmless microorganisms or pollen or from plumes of mold spores. Despite their shortcomings, particle detectors are useful for guiding troops away from areas that might pose a danger from a biological aerosol. They might also be deployed to indicate when more sensitive detectors should begin to analyze samples [*see box on next page*].

Overview/*Biodetectors*

- Biowarfare agents are colorless and odorless and could take days to cause symptoms. Accordingly, a society might not know it was under attack until it was too late to respond.
- Biologists and engineers are developing detectors consisting of chips that detect pathogens using antibodies or DNA. They are also coming up with devices that "sniff out" odors emitted by microbes or the additives used to make them into weapons.
- Public officials must decide how best to deploy the new bioweapons detectors; it would be impractical, for example, to put them on every street corner.

A Needle in a Haystack

SOME OF THE NEWEST biological weapons detectors can distinguish pathogens from benign microorganisms or other particles based on differences in their genetic makeup. Because DNA is located within microbes, the cells must first be broken open so their DNA can be extracted. Some devices, such as the GeneXpert system made by Cepheid in Sunnyvale, Calif., have built-in cell disrupters; others require a technician to isolate the DNA.



DNA-BASED BIOCHIP detects DNA from a pathogen by making a bridge of gold particles linking two electrodes. The bridge completes an electrical circuit, raising an alarm.

One of the first DNA chips, which was developed at Northwestern University, relies on the complementary nature of the two strands that constitute the DNA double helix. The DNA helix is like a twisted ladder in which each rung is composed of two subunits called bases. The ladder splits down the middle when genes are turned on or when a cell is copying its genes before dividing. Four bases make up the rungs of the helix: adenine (A), thymine (T), cytosine (C) and guanine (G). A always binds to T, and C always pairs with G. Knowing the sequence of bases from one strand—ATCGCC, for example—one can predict the complementary sequence of the other strand, in this case TAGCGG.

The sensing element of the Northwestern University system contains single strands of DNA that are complementary to a short sequence of DNA that is specific to a given pathogen. The strands are immobilized on a glass chip between two electrodes. When DNA from that particular pathogen enters the system, it sticks to, or hybridizes with, one end of the immobilized DNA. To detect this hybridization, a technician adds pieces of DNA

FRED RIX

COPYRIGHT 2002 SCIENTIFIC AMERICAN, INC.

Deploying the Defense

Deciding when—and where—to use biological warfare detectors may be the hardest part

A BIOLOGICAL ATTACK could occur anytime, anywhere. Madmen bent on killing as many people as possible could just as easily release a cloud of pathogens at a rural state fair as they could unleash a biological agent in an urban subway train during rush hour. (In the former case, however, they would have to pick an overcast day: bright sunlight kills most microbes.)

Since September 11, 2001, the fear of a terrorist attack has pervaded the thinking of events planners from New York City to Punxsutawney, Pa., which beefed up security this past Groundhog Day to foil possible attacks. Although the diversity and abundance of potential targets will make it impossible or impractical to protect all of them completely, properly deploying biological detectors could reduce the likelihood that the worst attacks would succeed.

Currently, biological agent detectors are too expensive and require too much maintenance to be placed on every street corner. Common sense dictates, however, that certain events or locations deserve tighter security because of their importance or the large number of potential victims there. The Capitol building and the Pentagon are at the heart of U.S. democracy and power and therefore deserve around-the-clock biological surveillance. Eventually technology may progress to the point where biological agent detectors will be reliable, cheap and self-sufficient enough to guard the municipal buildings of every major city.

Unfortunately, no biological agent detector available now can both distinguish harmful organisms from benign ones and monitor its surroundings constantly for pathogens. Some devices cannot collect samples automatically and require a human operator. Others can take samples mechanically, by sampling air or water, but are able to do so only when directed by an operator, who must acquire the samples at intervals to allow adequate time for analysis. Operators could take samples at set times—such as every hour or as soon as the previous sample was analyzed—but a cloud of biological agents could pass over an area or be dispersed in a matter of minutes. Taking samples at the wrong time could miss an attack.

U.S. ARMY'S Long Range Biological Standoff Detection System operates on board a Black Hawk helicopter. Such lidar-based particle detectors can be coupled to biochips that can distinguish particles of harmless microbes from those containing bioweapons.

Some detectors are linked to lidar systems or particle counters and collect samples only when a cloud of particles of the right size is present. Similar systems could be used to test the water that flows in the water mains that supply sensitive buildings: if the particle count in a water main spiked, the device would divert a sample of water for further analysis.

A system that could monitor its environment continuously, analyze samples rapidly and operate at low cost would be ideal, but such a system has yet to be perfected. In the meantime, epidemiologists and computer scientists have collaborated to create a database for monitoring the symptoms of patients who visit emergency rooms to detect the earliest signs of a biological attack. The protocol relies on handheld devices that physicians use to upload symptom information to a database that can pick up patterns of illness—such as an unusual number of flu-like illnesses outside flu season—that are consistent with the leading edge of a biological attack.

One such system—known as the Lightweight Epidemiology Advanced Detection and Emergency Response System (LEADERS)—has been used since 2000 to mine hospital databases in areas near major events such as political party conventions, the Super Bowl and the World Series. Mindful of the fact that most people do not go to the hospital when they think they have the flu, programmers are adding metrics into the LEADERS database such as sales of over-the-counter medications, sick-day tallies and tollbooth receipts (sick people are less likely to drive). Ideally, these databases would log patient information from all over the nation constantly so that attacks in the country could be detected early, no matter where, when or how they occur [see "The Vigilance Defense," on page 88]. *—R.C.*

LOS ALAMOS NATIONAL LABORATORY

COPYRIGHT 2002 SCIENTIFIC AMERICAN, INC.

that have gold particles tethered to them and that are complementary to the other end of the target DNA sequence. Where the gold-bearing DNA sequences bind, they complete an electrical circuit between the electrodes and raise an alarm.

Several other DNA-based detectors rely on the fact that specific sequences of DNA can be amplified through a process called the polymerase chain reaction (PCR). In this technique, scientists heat DNA so that the bonds between the two bases that make up each rung break and the two strands of DNA separate. Then they cool the solution and add two short pieces of DNA, called primers, that are designed to hybridize specifically to either end of the DNA sequence they are attempting to detect. Enzymes latch on to the primers and extend them, copying the initial two strands of DNA into four. Scientists can double the number of copies of the target DNA sequence each time they repeat the cycle until there is enough to detect.

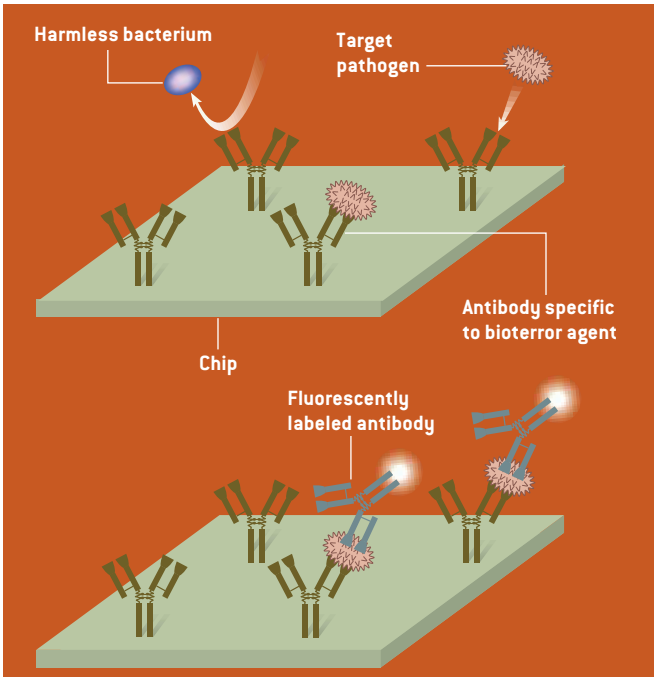
By incorporating fluorescent molecules in the newly synthesized pieces of DNA, researchers can monitor the amplification process as it progresses. Also available are machines called rapid thermal cyclers that complete each round of heating and cooling in less than a minute, allowing 30 doublings of very scarce DNA sequences to be accomplished within half an hour.

But the circuit- and PCR-based systems must be preloaded with reagents that are specific to particular pathogens, which means that users must guess correctly beforehand which pathogens a potential terrorist might choose. To circumvent this shortcoming, scientists at Ibis Therapeutics in Carlsbad, Calif., and Science Applications International Corporation in San Diego have developed a system called Triangulation Identification Genetic Evaluation of biological Risks (TIGER). Like many other DNA chips, TIGER amplifies target DNA using PCR. It is different, though, in that it employs primers that hybridize to a segment of DNA involved in controlling protein synthesis that is part of the basic machinery of all cells. TIGER can still be exquisitely sensitive because the sections between the primers are so highly variable that almost every microorganism has a unique sequence. Technicians can then analyze those amplified sequences using a mass spectrometer and compare them against a database of patterns from all known microorganisms to identify the agent.

DNA-based devices have their limitations, however. They cannot detect toxins, which have no DNA, and their half-hour reaction time makes them too slow to be used to alert people of an oncoming cloud of biowarfare pathogens in time for them to evacuate.

Canary in a Coal Mine

CHIPS BASED ON ANTIBODIES—Y-shaped molecules produced by the immune system that bind to specific target molecules on invaders—can surmount these hurdles. Because antibodies can detect molecules on the surfaces of microbes, no additional time is needed to break open the target cells. They can also ferret out toxins as well as whole microorganisms.



ANTIBODY-BASED CHIPS specifically bind pathogens, which are detected using other antibodies with fluorescent tails.

Antibodies are the heart of a biowarfare detection system designed by the U.S. Naval Research Laboratory called Raptor. The system is a so-called sandwich assay: target pathogens stick to antibodies on the chip and are detected when they are sandwiched between another layer of antibodies labeled with fluorescent dyes. Raptor can pick up on several pathogens at once because it can accommodate spots of several types of antibodies, each specific to a different bioweapon. The Origen system from Igen in Gaithersburg, Md., also detects pathogens using a sandwich assay, but instead of fluorescent dyes it relies on a compound that emits a burst of light when exposed to an electric field. The light is brighter than normal fluorescence, allowing the analysis of samples that contain only a few pathogens. Furthermore, one of the antibodies is tethered to a surface that allows the target pathogens to be concentrated before detection.

At Surface Logix, we have collaborated with Radiation Monitoring Devices in Watertown, Mass., to develop technology that can be used to pick up pathogens on a continuous basis. The machine, which can be connected to an air sampler,

FRED RIX

THE AUTHOR

ROCCO CASAGRANDE is a scientist at the biotechnology company Surface Logix in Brighton, Mass., where he designs and tests biological agent detectors. He received his Ph.D. from the Massachusetts Institute of Technology in 2001. Casagrande has consulted for the U.S. Defense Threat Reduction Agency and is a member of the Controlling Dangerous Pathogens Group at the University of Maryland. He is also on the roster of inspectors of the United Nations Monitoring, Verification and Inspection Commission, which is charged with ensuring Iraq's biological and chemical weapons disarmament.

COPYRIGHT 2002 SCIENTIFIC AMERICAN, INC.

mixes any particles present in the sampled air with a solution of microscopic magnetic beads. Each bead is coated with fluorescently labeled antibodies that bind to a particular microbe.

The sample stream containing the beads flows down a microscopic channel about the width of a human hair, where it meets a clean stream free of microorganisms. The clean stream and the sample stream flow side by side without mixing until they hit a fork in the channel. A magnet placed just before the fork pulls the magnetic beads—and any pathogens bound to them—into the clean stream. That stream then flows into a detector that registers the presence of pathogens by their fluorescence.

A major advantage of our system is that it removes target pathogens from the thousands of harmless organisms present in a given sample. Smoke and other environmental contaminants in the sample do not affect detection, because the microbeads are pulled into the clean stream before the fluorescence-detection step. In addition, the machine accepts samples from the environment constantly and analyzes them in real time.

Other systems use antibodies to capture passing pathogens onto vibrating devices such as quartz crystals, thin membranes or microscopic cantilevers. As these devices capture pathogens, they become weighed down, which slows their vibrations. This change is detectable by electronics.

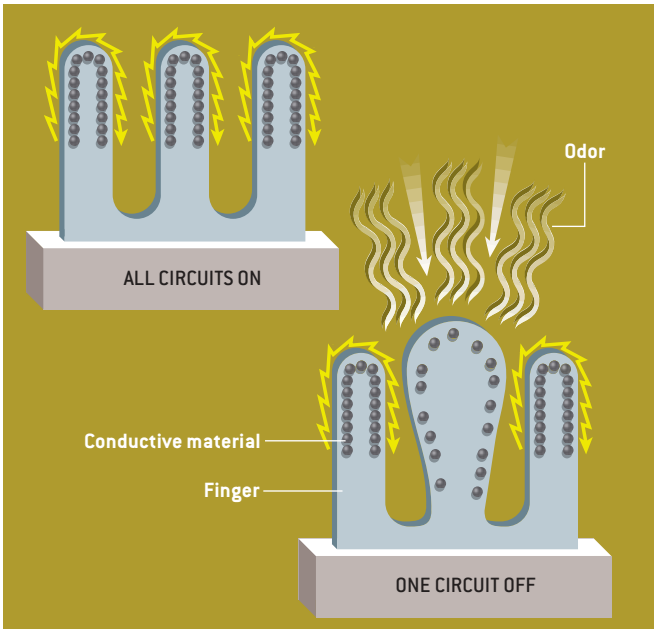
Sniffing Out Invaders

THE DEVICES MENTIONED in this article are either available now or expected to be within the next few years. But newer, more powerful technologies are being developed all the time.

So-called electronic noses—which are currently used to spot explosives and chemical weapons—are being adapted to sniff out biological bombs. One such device, the Cyranose, made by Cyrano Sciences in Pasadena, Calif., contains an array of pegs made of slightly different polymers. Each polymer peg has a specific capacity for absorbing a particular chemical, which causes it to swell. The pegs contain flecks of material that conduct electricity. When the pegs are not swollen, the flecks are close enough to one another to conduct electricity; as they swell, the flecks become separated, breaking the circuit and yielding a positive signal. The pattern of broken circuits is different for each odor. Researchers are devising noses that can pick up metabolites given off by dangerous bacteria or by chemicals such as stabilizers that are often part of biological weapons. The hope is to find a pattern unique to a biological agent.

In a highly innovative approach, BCR Diagnostics in Jamestown, R.I., uses dormant forms of bacteria called spores to tip off the presence of bioweapons. When bacteria enter the detector, their normal metabolism cleaves an inactive nutrient into an active one, allowing the detector's spores to germinate. Because the spores have been genetically modified to emit light as they undergo this transformation, the detector registers the presence of the pathogen. Unfortunately, this device detects the presence of all bacteria, whether harmful or not. But it could be adapted by specially designing inactive nutrients that would be converted to active ones only by the types of bacteria most likely to be used in bioweapons.

A clever terrorist could fool even the best biodetector, however, by genetically engineering an otherwise harmless organism to produce deadly toxins. The ideal detector would respond to the presence of a biological weapon exactly as its target would, but more quickly. To this end, the Defense Advanced Research Projects Agency is currently supporting biodetector research involving living cells from humans, animals or plants. The idea behind this kind of detector is that a human pathogen must be harmful to at least one type of human cell; measuring the extent of cell death in the detector would indicate the presence of a harmful organism in the environment.



ELECTRONIC NOSE has polymer fingers that swell when they sense a particular odor. The swelling separates bits of conductive material lodged within the fingers and breaks an electrical circuit, triggering an alarm.

Although biological weapons are horrifying, no country or terrorist group has yet wielded them to kill thousands of people. Biodetectors can in principle help protect populations against such an unlikely event, but they can also fill other roles. Pathogen detectors can be deployed to identify contaminated food or to diagnose infectious diseases in a doctor's office. Devices that measure cellular responses can also be used evaluate the susceptibility of cancer cells to various drugs, allowing scientists to identify potential therapeutics more rapidly. In this way, it might be possible to turn shields—instead of swords—into plowshares. SA

MORE TO EXPLORE

America's Achilles' Heel: Nuclear, Biological and Chemical Terrorism and Covert Attack. Richard A. Falkenrath, Robert D. Newman and Bradley A. Thayer. MIT Press, 1998.

Biological Warfare: Modern Offense and Defense. Edited by Raymond A. Zilinskas. Lynne Rienner Publishers, Boulder, Colo., 1999.

Information on the TopOff exercise and Dark Winter is at **www.house.gov/reform/ns/web_resources/briefing_memo_july_23.htm**

FRED RIX

COPYRIGHT 2002 SCIENTIFIC AMERICAN, INC.