tising space in *Genetics*, the journal she edits, to plug her tutoring software. "I wouldn't have that bully pulpit if I had just taught," she says. Jones and the other fellows will have a chance to convert other high-powered researchers at meetings with Hughes investigators. The institute will assess the program before deciding whether to repeat it in 2006.

–ERIK STOKSTAD

U.S. ENVIRONMENT

Report Takes Stock of Knowns and Unknowns

The United States spends more than $120 billion a year on protecting ecosystems, but the information used to evaluate such efforts is often inadequate or of questionable relevance, say ecologists and policy experts. According to one environmentalist, it's like monitoring a sick patient by measuring fingernail length. A new report—*The State of the Nation's Ecosystems*, published 24 September by the nonpartisan Heinz Center in Washington, D.C.—tries to provide the missing data and point out where better measures are needed.

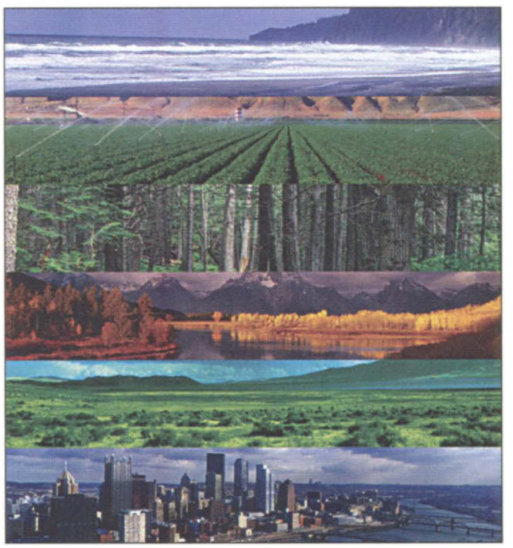
The Heinz report (www.heinzctr.org/ecosystems) aspires to be the Dow Jones Industrial Average of the environment. But don't expect to see it published next to the latest stock prices; half of its "ecosystem indicators" can't be measured yet. And for those that can be measured, the center is not saying whether the results represent good or bad news, because it wants to steer away from opinion.

Some environmentalists say such rigid neutrality masks the dire straits of certain ecosystems. But the report's authors insist that their approach is an essential starting point for protecting the environment. The authors also worked to build consensus among people with a range of viewpoints. As with economic indicators, they say, the goal is to start with widely accepted data, which can lead to a debate on policies to change the status quo.

The $3.7 million report was conceived in 1995 by the White House Office of Science and Technology Policy, which asked the Heinz Center to complete it. Its funders run the ideological gamut from International Paper to Defenders of Wildlife, and its 150 authors come from universities, environmental groups, industry, and government. About 100 reviewers of a prototype report in 1999 (*Science*, 10 December 1999, p. 2071) helped the team's seven committees compile government data into 10 national indicators plus 93 other indicators tailored to fit six broad ecosystem types.

Despite all the number crunching, the 270-page report is most striking for what it lacks. "Half the report is empty," admits William Clark, chair of the report's design committee and a professor of international science policy at Harvard University's John F. Kennedy School of Government in Cambridge, Massachusetts. Missing data are marked by bleak gray boxes that say, "Data Not Adequate," meant to prod monitoring programs to fill the gaps. For example, participants agreed that the degree of human alteration is an important ecosystem indicator but say there is no widely accepted way to measure it.

The available indicators organize and add precision to a welter of existing data. For example, the report points out that the four major U.S. rivers carry three times as much nitrate per year as in 1955. A fifth of native animal species are faced with serious decline. Three-fifths of estuaries are contaminated. On the other hand, 85% of streams meet human health standards. Moreover, agricultural production has doubled since the 1950s, and land threatened by erosion has declined by a third since 1985.



Sea to shining sea. A new report identifies environmental health indicators for six broad ecosystem types.

CREDIT: THE H. JOHN HEINZ III CENTER FOR SCIENCE, ECONOMICS AND THE ENVIRONMENT

"Anyone could do a list that would make everything look good or everything look bad," Clark says. The report's authors sought to avoid the criticism, often heaped on past assessments, that their measures are biased. The Heinz report's indicators are accepted by all participants.

But some environmentalists say the focus on consensus is the report's greatest weakness. "Because the emphasis was on producing a report that was consensus-driven, they had to focus on the margins of what most scientists would have looked at," says Dominick DellaSala of the World Wildlife Fund. He quit one of the report committees, claiming that its indicator of forest fragmentation downplays the extent to which forests are broken up by roads, power lines, and development.

Observers' initial reactions were mixed. The report "is the first to employ a comprehensive set of indicators integrating biophysical and sociocultural measures," says ecologist Bruce Wilcox of the University of Hawaii, Honolulu, who edits the journal *Ecosystem Health*. David Rapport of the University of Guelph in Ontario, Canada, however, is disappointed. "No attempt is made … to relate human activities to the changes in American ecosystems, and no attempt is made to evaluate the health of U.S. ecosystems," he says. But Chet Boruff of Farmers National Marketing Group in Moline, Illinois, defends the report's neutrality: "That's the best way to build understanding … and to come up with a report that is unbiased."

–BEN SHOUSE

Ben Shouse is a writer in Santa Cruz, California.

ANIMAL RESEARCH

Coulston Chimps Head to Retirement

The beleaguered Coulston Foundation, formerly the largest chimpanzee research facility in the United States, is no longer in the primate research business. On 16 September the Florida-based Center for Captive Chimpanzee Care took over Coulston's Alamogordo, New Mexico, facility. The new caretaker for the 266 chimpanzees and 61 monkeys plans to retire the animals from research, eventually relocating many to a sanctuary in Florida.

The Coulston Foundation had long been dogged by complaints about and government investigations into its animal care practices. Last summer the National Institutes of Health (NIH) let lapse the foundation's Animal Welfare Assurance, which is required for government-supported animal research (*Science*, 24 August 2001, p. 1415). Faced with mounting debts and few customers, the foundation's president, Frederick Coulston, agreed to sell its property and equipment to the Center for Captive Chimpanzee Care (CCCC), for $3.7 million, and also donate the remaining animals. About two dozen Coulston-owned chimpanzees are housed at other research facilities, but Carol Noon, president of CCCC, expects them to be retired as well.

Toxicologist and millionaire Coulston founded the nonprofit in 1993. Despite complaints of negligent and unsafe practices from animal-rights groups, by 1998 the foundation was the nation's largest chimpanzee research facility, housing more than 600 chimps. The foundation's troubles mounted as a series of inquiries by the U.S. Department of Agriculture (USDA) and the Food and Drug Administration found Coul-

ston in violation of the Animal Welfare Act and Good Laboratory Practices regulations. In a settlement with USDA in 1999, the foundation, without admitting guilt, agreed to give up half of its chimps.

As part of that agreement, NIH in May 2000 took custody of 288 of Coulston's animals, many of which had been infected with HIV or hepatitis C. In May 2001, NIH awarded a contract to Charles River Laboratories to care for the animals at a primate facility at Holloman Air Force Base outside Alamogordo, a property Coulston had been managing. A month later, NIH allowed Coulston's Animal Welfare Assurance to lapse. That left Coulston with more than 250 chimpanzees at its main Alamogordo facility but no possibility of government funding and few private customers.

Looking forward. The Coulston Foundation's chimpanzees will be retired from research.

In December, a local bank filed suit to recover $1.2 million in unpaid loans (*Science*, 18 January, p. 421). Facing mounting debts, Coulston began negotiations with CCCC last spring. The center announced its agreement with Coulston last week. For now, the chimpanzees and monkeys will remain at the Alamogordo facility, Noon says. But the Arcus Foundation in Kalamazoo, Michigan, which donated the $3.7 million for the Coulston purchase, has said it will help fund additional construction at CCCC's sanctuary in Florida.

John Strandberg, head of the National Center for Research Resources at NIH, says the animals' retirement should not affect researchers. "There are enough chimpanzees in the program now to meet needs," he says. "I definitely think it's a positive development. These animals needed a long-term-care solution, and the Center for Captive Chimpanzee Care is able to provide that."

Coulston spokesperson Don McKinney says that the Coulston Foundation will continue to exist but that it "will be taking a different research direction, closer to pure science." He declined to elaborate.

–GRETCHEN VOGEL

CREDIT: (TOP) CRYSTAL MILLER/SPIEGEL/AAVS

COMPUTER SECURITY

Crucial Cipher Flawed, Cryptographers Claim

It was supposed to be as secure as a bank vault: a cryptographic algorithm that would make documents unintelligible to prying eyes for the foreseeable future. But two cryptographers say the vault, the Advanced Encryption Standard (AES), has a hole in it. Although some of their colleagues doubt the validity of their analysis, the cryptographic community is on edge, wondering whether the new cipher can withstand a future assault.

"It's nerve-wracking for me that this stuff is going on," says William Burr, the manager of the Security Technology group at the National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland. "It's very worrisome if [the analysis] holds up, but it may not hold up."

Two years ago, NIST selected an algorithm to replace the aging Digital Encryption Standard. DES, the national standard for a quarter-century, was arguably the most widely used encryption algorithm in the world. But when it began to show its age, NIST held a competition to determine the next standard (*Science*, 19 May 2000, p. 1161). Rijndael, an elegant algorithm created by two Belgians, Vincent Rijmen of the Katholieke Universiteit Leuven and Joan Daemen of Proton World International, a company that makes smart cards, won the contest and became the AES (*Science*, 6 October 2000, p. 25).

Now, attacks aimed at the heart of Rijndael and other algorithms point to a possible weakness. Cryptographers Nicolas Courtois, who works for technology corporation SchlumbergerSema in Louveciennes, France, and Josef Pieprzyk of Macquarie University in Sydney, Australia, believe they have undermined the algorithms by rewriting their "S-boxes."

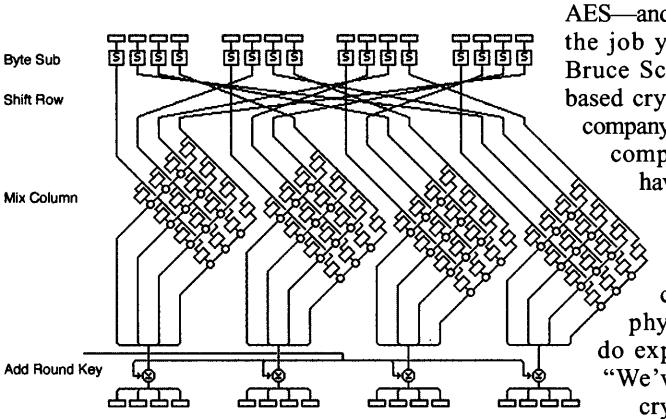
S-boxes are a crucial element in many ciphers. An S-box adds unpredictability to an algorithm. It takes a string of ones and zeros and returns a different set, turning small changes in input into large changes in output—a boost that makes the algorithm much more difficult to crack. Probing for weaknesses, Courtois and Pieprzyk rewrote Rijndael's S-boxes as a system of equations that a cracker must solve to break the cipher. "[Each S-box] can be described by a small system of equations," says Courtois. "Nobody thought it would matter."

But it does matter. Earlier this year, cryptographers Sean Murphy and Matt Robshaw of the Royal Holloway University of London showed that the S-boxes can be reformulated in a way that Courtois and Pieprzyk exploited to make their attack a force to be reckoned with. All told, Courtois and Pieprzyk believe that they have an attack of order 2^{100}: That is, it takes roughly 2^{100} operations to crack the cipher, significantly less than the 2^{128} to 2^{256} operations needed to try every combination.

Even if Courtois and Pieprzyk are correct, AES won't crumble overnight. The fastest computers can mount attacks of perhaps order 2^{70}, Burr says: "With 2^{100}, we might not be able to verify the attack for the next 70 years, maybe more." Still, he says, a theoretically sound attack would be a "very, very disturbing proposition," because attacks get refined over time and computers are speeding up exponentially.

Some analysts think there's nothing to fret about. Don Coppersmith, a cryptographer at IBM in Yorktown, New York, and one of the designers of DES, claims to have found a flaw in the analysis: Courtois and Pieprzyk miscounted the number of equations, he believes. But Courtois says the criticism does not apply to the latest version of the paper, which will be presented in December at the Asiacrypt 2002 conference.

Barring an obvious mathematical error, though, it might take cryptographers years to determine whether the attack is worrisome. The only way to prove that the algorithm works, Courtois says, is to use it to crack AES—and computers aren't up to the job yet. Meanwhile, says Bruce Schneier, a Minnesota-based cryptographer at security company Counterpane Systems, computer-security experts have no way of knowing which attacks pose true threats and which are phantoms. "How could you do particle physics if you couldn't do experiments?" he asks. "We've entered an era of cryptanalysis where you can't verify attacks."



Scrambled. Simplifying the math behind AES might leave the encryption algorithm vulnerable to attack.

–CHARLES SEIFE