he calls "performers," to actually hunt for the errant circuits; and a final group to judge the results.

To fabricate the test chips, Collins chose the Information Sciences Institute at the University of Southern California, Los Angeles. He picked MIT's Lincoln Laboratory to engineer whatever sneaky insertions they could devise, and he tapped Johns Hopkins University Applied Physics Laboratory, in Laurel, Md., to come up with a way to compare and assess the performers' results.

The three performers are Raytheon, Luna Innovations, and Xradia. None of the teams would speak on the record, but their specialties offer some clues to their approach. Xradia, in Concord, Calif., builds nondestructive X-ray microscopes used widely in the semiconductor industry, so it may be looking at a new method of inspecting chips based on soft X-ray tomography, Stanford's Pease suggests. Soft X-rays are powerful enough to penetrate the chip but not strong enough to do irreversible damage.

Luna Innovations, in Roanoke, Va., specializes in creating antitamper features for FPGAs. Princeton's Lee suggests that Luna's approach may involve narrowing down the number of possible unspecified functions. "There are ways to determine where such hardware would be inserted," she says. "Where could they gather the most information? Where would they be least likely to be noticed? That is what they're looking for." She compares chip security to a barricaded home. The front door and windows might offer vault-like protection, but there might be an unknown window in the basement. The Luna researchers, she speculates, may be looking for the on-chip equivalent of the basement window.

Raytheon, of Waltham, Mass., has expertise in hardware and logic testing, says Collins. He believes the company will use a more complex version of a technique called Boolean equivalence checking to analyze what types of inputs will generate certain outputs. Normally, applying specific inputs to a circuit will result in specific, predictable outputs, just as hitting a light switch should always cause the light to turn off. "Now look at that process in reverse," says Collins. Given a certain output (the lights go out), engineers can reconstruct what made it happen (someone hit a switch). Collins says this could help avoid cycling through infinite combinations of inputs to find a single fatal response.

In January, the performers were given a set of four test chips, each containing an unknown (to them) number of malicious insertions. Along with a thorough description of the chips, Collins says, "we told them precisely what the circuits were supposed to be."

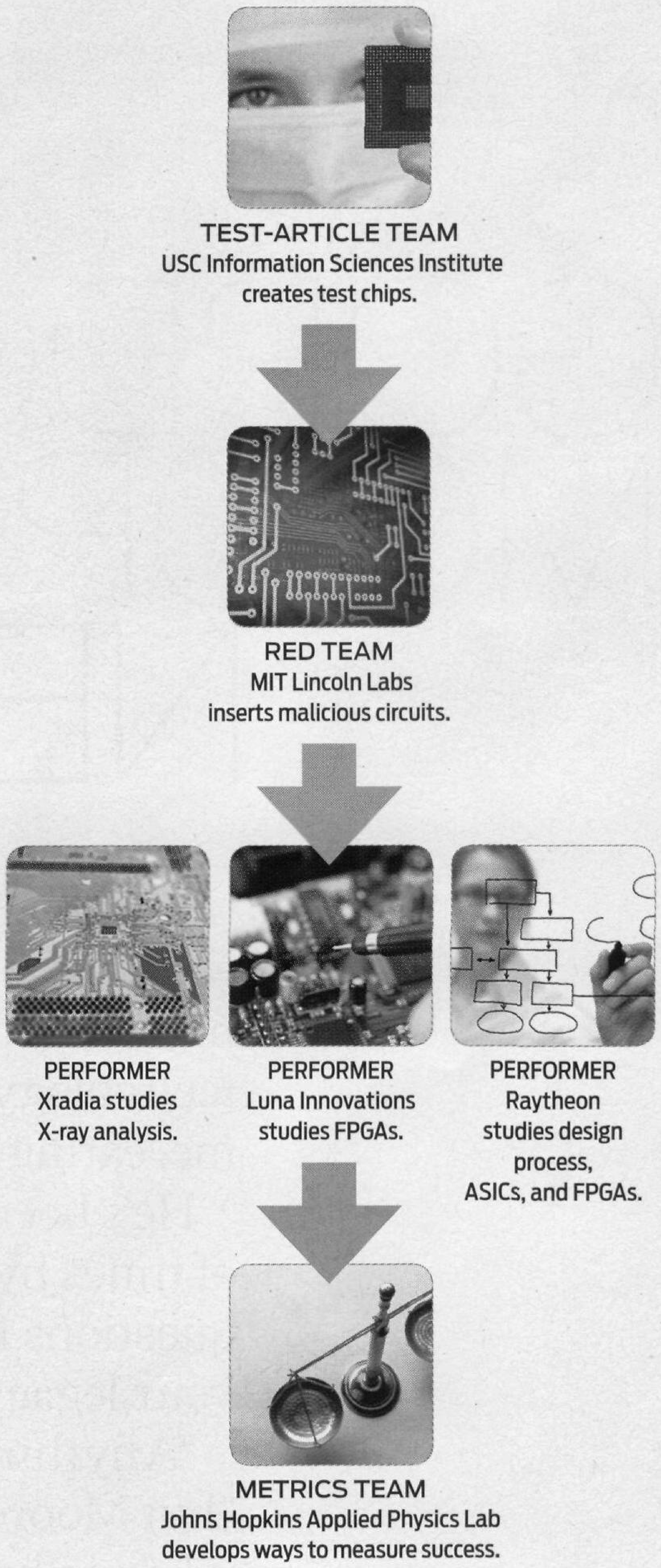
Each team's success will be gauged by the number of malicious insertions it can spot. The goal is a 90 percent detection rate, says Collins, with a minimum of false positives. The teams will also have to contend with red herrings: to trip them up, the test set includes fully functioning, uncompromised chips. By the end of this month, the performers will report back to DARPA. After Johns Hopkins has tallied the results, the teams will get a second set of test chips, which they'll have to analyze by the end of the year. Any performer that doesn't pass muster will be cut from the program, while the methods developed by the successful ones will be developed further. By the program's end in 2010, Collins hopes to have a scientifically verifiable method to categorically authenticate a circuit. "There's not going to be a DARPA seal of approval on them," says Collins, but both the Army and the Air Force have already expressed interest in adopting whatever technology emerges.

Meanwhile, other countries appear to be awakening to the chip threat. At a January hearing, a U.S. House Committee on Foreign Affairs addressed Pakistan's ongoing refusal to let the United States help it secure its nuclear arsenal with American technology. Pakistan remains reluctant to allow such intervention, citing fears that the United States would use the opportunity to cripple its weapons with—what else?—a kill switch. ❑

ISTOCKPHOTO (6)

SCAVENGER HUNT

DARPA'S PROGRAM has formed teams to test chip integrity. USC's group creates the chips, which MIT's group then compromises with unknown additions. The "performers," Xradia, Luna Innovations, and Raytheon, are supposed to find the malicious alterations. And the Johns Hopkins group judges the results. The program's three phases get progressively harder, with the number of insertions increasing and the testing time decreasing.



TEST-ARTICLE TEAM
USC Information Sciences Institute
creates test chips.

RED TEAM
MIT Lincoln Labs
inserts malicious circuits.

PERFORMER
Xradia studies
X-ray analysis.

PERFORMER
Luna Innovations
studies FPGAs.

PERFORMER
Raytheon
studies design
process,
ASICs, and FPGAs.

METRICS TEAM
Johns Hopkins Applied Physics Lab
develops ways to measure success.

TO PROBE FURTHER For a comprehensive look into the failure of the Syrian radar, see "Cyber-Combat's First Shot," Aviation Week & Space Technology, *26 November 2007 by David A. Fulghum, Robert Wall, and Amy Butler. For more on the DARPA program and on the kill-switch debate, go to http://spectrum.ieee.org/may08/chiptrust.*