Collins notes that many defense contractors rely heavily on field-programmable gate arrays (FPGAs)—a kind of generic chip that can be customized through software. While a ready-made FPGA can be bought for $500, an application-specific IC, or ASIC, can cost anywhere from $4 million to $50 million. "If you make a mistake on an FPGA, hey, you just reprogram it," says Collins. "That's the good news. The bad news is that if you put the FPGA in a military system, someone else can reprogram it."

Almost all FPGAs are now made at foundries outside the United States, about 80 percent of them in Taiwan. Defense contractors have no good way of guaranteeing that these economical chips haven't been tampered with. Building a kill switch into an FPGA could mean embedding as few as 1000 transistors within its many hundreds of millions. "You could do a lot of very interesting things with those extra transistors," Collins says.

The rogue additions would be nearly impossible to spot. Say those 1000 transistors are programmed to respond to a specific 512-bit sequence of numbers. To discover the code using software testing, you might have to cycle through every possible numerical combination of 512-bit sequences. That's 13.4×10^{153} combinations. (For perspective, the universe has existed for about 4×10^{17} seconds.) And that's just for the 512-bit number—the actual number of bits in the code would almost certainly be unknown. So you'd have to apply the same calculations to all possible 1024-bit numbers, and maybe even 2048-bit numbers, says Tim Holman, a research associate professor of electrical engineering at Vanderbilt University, in Nashville. "There just isn't enough time in the universe."

Those extra transistors could create a kill switch or a backdoor in any chip, not just an FPGA. Holman sketches a possible scenario: suppose those added transistors find their way into a networking chip used in the routers connecting the computers in your home, your workplace, banks, and military bases with the Internet. The chip functions perfectly until it receives that 512-bit sequence, which could be transmitted from anywhere in the world. The sequence prompts the router to hang up. Thinking it was the usual kind of bug, tech support would reset the router, but on restart the chip would again immediately hang up, preventing the router from connecting to the outside world. Meanwhile, the same thing would be happening to similarly configured routers the world over.

The router scenario also illustrates that the nation's security and economic well-being depend on shoring up not just military chips but also commercial chips. An adversary who succeeded in embedding a kill switch in every commercial router could devastate national security without ever targeting the Defense Department directly.

A kill switch or backdoor built into an encryption chip could have even more disastrous consequences. Today encoding and decoding classified messages is done completely by integrated circuit—no more Enigma machine with its levers and wheels. Most advanced encryption schemes rely on the difficulty that computers have in factoring numbers containing hundreds of digits; discovering a 512-bit type of encryption would take some machines up to 149 million years. Encryption that uses the same code or key to encrypt and decrypt information—as is often true—could easily be compromised by a kill switch or a backdoor. No matter what precautions are taken at the programming level to safeguard that key, one extra block of transistors could undo any amount of cryptography, says John East, CEO of Actel Corp., in Mountain View, Calif., which supplies military FPGAs.

"Let's say I can make changes to an insecure FPGA's hardware," says East. "I could easily put a little timer into the circuit. The timer could be programmed with a single command: 'Three weeks after you get your configuration, forget it.' If the FPGA were to forget its configuration information, the entire security mechanism would be disabled."

Alternately, a kill switch might be programmed to simply shut down encryption chips in military radios; instead of scrambling the signals they transmit, the radios would send their messages in the clear, for anybody to pick up. "Just like we figured out how the Enigma machine worked in World War II," says Stanford's Adler, "one of our adversaries could in principle figure out how our electronic Enigma machines work and use that information to decode our classified communications."

Chip alteration can even be done after the device has been manufactured and packaged, provided the design data are available, notes Chad Rue, an engineer with FEI, based in Hillsboro, Ore., which makes specialized equipment for chip editing (albeit for legitimate reasons). FEI's circuit-editing tools have been around for 20 years, Rue says, and yet "chip designers are still surprised when they hear what they can do."

Skilled circuit editing requires electrical engineering know-how, the blueprints of the chip, and a $2 million refrigerator-size piece of equipment called a focused-ion-beam etching machine, or FIB. A FIB shoots a stream of ions at precise areas on the chip, mechanically milling away tiny amounts of material. FIB lab workers refer to the process as microsurgery, with the beam acting like a tiny scalpel. "You can remove material, cut a metal line, and make new connections," says Rue. The process can take from hours to several days. But the results can be astonishing: a knowledgeable technician can edit the chip's design just as easily as if he were taking "an eraser and a pencil to it," says Adler.

Semiconductor companies typically do circuit editing when they're designing and debugging prototypes. Designers can make changes to any level of the chip's wiring, not just the top. "It's not uncommon to dig through eight different layers to get to the intended target," says Rue. The only thing you can't do with a FIB is add extra transistors. "But we can reroute signals to the transistors that are already there," he says. That's significant because chips commonly contain large blocks of unused circuitry, leftovers from previous versions of the design. "They're just along for the ride," Rue says. He thinks it would be possible to use a FIB to rewire a chip to make use of these latent structures. To do so, an adversary would need a tremendous amount of skill with digital circuitry and access to the original design data. Some experts find the idea too impractical to worry about. But an adversary with unlimited funds and time—exactly what the Defense Science Board warned of—could potentially pull it off, Rue says.

In short, the potential for tinkering with an integrated circuit is almost limitless, notes Princeton's Lee. "The hardware design process has many steps," she says. "At each step, you could do something that would make a particular part of the IC fail."

CLEARLY, THE COMPANIES participating in the Trust in IC program have their work cut out for them. As Collins sees it, the result has to be a completely new chip-verification method. He's divided up the Trust participants into teams: one group to create the test chips from scratch; another to come up with malicious insertions; three more groups, which