SEMICONDUCTOR OFFSHORING dates back to the 1960s, when U.S. chip makers began moving the labor-intensive assembly and testing stages to Singapore, Taiwan, and other countries with educated workforces and relatively inexpensive labor.

Today only Intel and a few other companies still design and manufacture all their own chips in their own fabrication plants. Other chip designers—including LSI Corp. and most recently Sony—have gone "fabless," outsourcing their manufacturing to offshore facilities known as foundries. In doing so, they avoid the huge expense of building a state-of-the-art fab, which in 2007 cost as much as US $2 billion to $4 billion.

Well into the 1970s, the U.S. military's status as one of the largest consumers of integrated circuits gave it some control over the industry's production and manufacturing, so the offshoring trend didn't pose a big problem. The Pentagon could always find a domestic fab and pay a little more to make highly classified and mission-critical chips. The DOD also maintained its own chip-making plant at Fort Meade, near Washington, D.C., until the early 1980s, when costs became prohibitive.

But these days, the U.S. military consumes only about 1 percent of the world's integrated circuits. "Now," says Coleman, "all they can do is buy stuff." Nearly every military system today contains some commercial hardware. It's a pretty sure bet that the National Security Agency doesn't fabricate its encryption chips in China. But no entity, no matter how well funded, can afford to manufacture its own safe version of every chip in every piece of equipment.

The Pentagon is now caught in a bind. It likes the cheap, cutting-edge devices emerging from commercial foundries and the regular leaps in IC performance the commercial sector is known for. But with those improvements comes the potential for sabotage. "The economy is globalized, but defense is not globalized," says Coleman. "How do you reconcile the two?"

In 2004, the Defense Department created the Trusted Foundries Program to try to ensure an unbroken supply of secure microchips for the government. DOD inspectors have now certified certain commercial chip plants, such as IBM's Burlington, Vt., facility, as trusted foundries. These plants are then contracted to supply a set number of chips to the Pentagon each year. But Coleman argues that the program blesses a process, not a product. And, she says, the Defense Department's assumption that onshore assembly is more secure than offshore reveals a blind spot. "Why can't people put something bad into the chips made right here?" she says.

Three years ago, the prestigious Defense Science Board, which advises the DOD on science and technology developments, warned in a report that the continuing shift to overseas chip fabrication would expose the Pentagon's most mission-critical integrated circuits to sabotage. The board was especially alarmed that no existing tests could detect such compromised chips, which led to the formation of the DARPA Trust in IC program.

Where might such an attack originate? U.S. officials invariably mention China and Russia. Kenneth Flamm, a technology expert at the Pentagon during the Clinton administration who is now a professor at the University of Texas at Austin, wouldn't get that specific but did offer some clues. Each year, secure government computer networks weather thousands of attacks over the Internet. "Some of that probing has come from places where a lot of our electronics are being manufactured," Flamm says. "And if you're a responsible defense person, you would be stupid not to look at some of the stuff they're assembling, to see how else they might try to enter the network."

John Randall, a semiconductor expert at Zyvex Corp., in Richardson, Texas, elaborates that any malefactor who can penetrate government security can find out what chips are being ordered by the Defense Department and then target them for sabotage. "If they can access the chip designs and add the modifications," Randall says, "then the chips could be manufactured correctly anywhere and still contain the unwanted circuitry."

SO WHAT'S THE BEST WAY to kill a chip? No one agrees on the most likely scenario, and in fact, there seem to be as many potential avenues of attack as there are people working on the problem. But the threats most often mentioned fall into two categories: a kill switch or a backdoor.

A kill switch is any manipulation of the chip's software or hardware that would cause the chip to die outright—to shut off an F-35's missile-launching electronics, for example. A backdoor, by contrast, lets outsiders gain access to the system through code or hardware to disable or enable a specific function. Because this method works without shutting down the whole chip, users remain unaware of the intrusion. An enemy could use it to bypass battlefield radio encryption, for instance.

Depending on the adversary's degree of sophistication, a kill switch might be controlled to go off at a set time, under certain circumstances, or at random. As an example of the latter, Stanford electrical engineering professor Fabian Pease muses, "I'd nick the [chip's] copper wiring." The fault, almost impossible to detect, would make the chip fail early, due to electromigration: as current flowed through the wire, eventually the metal atoms would migrate and form voids, and the wire would break. "If the chip goes into a defense satellite, where it's supposed to work for 15 years but fails after six months, you have a very expensive, inoperative satellite," Pease says.

But other experts counter that such ideas ignore economic realities. "First and foremost, [the foundries] want to make sure their chips work," says Coleman. "If a company develops a reputation for making chips that fail early, that company suffers more than anyone else."

A kill switch built to be triggered at will, as was allegedly incorporated into the European microprocessors, would be more difficult and expensive to pull off, but it's also the more likely threat, says David Adler, a consulting professor of electrical engineering at Stanford, who was previously funded by DARPA to develop chip-testing hardware in an unrelated project.

To create a controlled kill switch, you'd need to add extra logic to a microprocessor, which you could do either during manufacturing or during the chip's design phase. A saboteur could substitute one of the masks used to imprint the pattern of wires and transistors onto the semiconductor wafer, Adler suggests, so that the pattern for just one microchip is different from the rest. "You're printing pictures from a negative," he says. "If you change the mask, you can add extra transistors."

Or the extra circuits could be added to the design itself. Chip circuitry these days tends to be created in software modules, which can come from anywhere, notes Dean Collins, deputy director of DARPA's Microsystems Technology Office and program manager for the Trust in IC initiative. Programmers "browse many sources on the Internet for a component," he says. "They'll find a good one made by somebody in Romania, and they'll put that in their design." Up to two dozen different software tools may be used to design the chip, and the origin of that software is not always clear, he adds. "That creates two dozen entry points for malicious code."