THE HUNT FOR THE KILL SWITCH

ARE CHIP MAKERS BUILDING ELECTRONIC TRAPDOORS IN KEY MILITARY HARDWARE? THE PENTAGON IS MAKING ITS BIGGEST EFFORT YET TO FIND OUT *BY SALLY ADEE*

LAST SEPTEMBER, Israeli jets bombed a suspected nuclear installation in northeastern Syria. Among the many mysteries still surrounding that strike was the failure of a Syrian radar—supposedly state-of-the-art—to warn the Syrian military of the incoming assault. It wasn't long before military and technology bloggers concluded that this was an incident of electronic warfare—and not just any kind.

Post after post speculated that the commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden "backdoor" inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips' function and temporarily blocked the radar.

That same basic scenario is cropping up more frequently lately, and not just in the Middle East, where conspiracy theories abound. According to a U.S. defense contractor who spoke on condition of anonymity, a "European chip maker" recently built into its microprocessors a kill switch that could be accessed remotely. French defense contractors have used the chips in military equipment, the contractor told *IEEE Spectrum*. If in the future the equipment fell into hostile hands, "the French wanted a way to disable that circuit," he said. *Spectrum* could not confirm this account independently, but spirited discussion about it among researchers and another defense contractor last summer at a military research conference reveals a lot about the fever dreams plaguing the U.S. Department of Defense (DOD).

Feeding those dreams is the Pentagon's realization that it no longer controls who manufactures the components that go into its increasingly complex systems. A single plane like the DOD's next generation F-35 Joint Strike Fighter, can contain an "insane number" of chips, says one semiconductor expert familiar with that aircraft's design. Estimates from other sources put the total at several hundred to more than a thousand. And tracing a part back to its source is not always straightforward. The dwindling of domestic chip and electronics manufacturing in the United States, combined with the phenomenal growth of suppliers in countries like China, has only deepened the U.S. military's concern.

Recognizing this enormous vulnerability, the DOD recently launched its most ambitious program yet to verify