Fake chips threaten military

September 14 2010, By Steve Johnson

A growing deluge of millions of counterfeit chips is posing peril to the military and the general public -- and perhaps nothing illustrates it better than a scheme federal prosecutors recently revealed that stretched from Southern California to Silicon Valley.

Mustafa Aljaff and Neil Felahy, a Newport Beach pair indicted in October, have admitted importing from China more than 13,000 bogus chips altered to resemble those from legitimate companies, including Intel, Atmel, Altera and National Semiconductor. Among those buying the chips was the U.S. Navy.

It wasn't the first time the military has been hoodwinked. Separate studies this year by the Commerce Department and the Government Accountability Office concluded that the armed forces -- which use chips in everything from communications and radar systems to warplanes and missiles -- is alarmingly vulnerable to fakes.

Commerce officials partly blamed the Iraq and Afghanistan wars for diminishing the supplies of chips the military normally uses for equipment repairs and forcing it to rely on questionable dealers for replacement parts. Moreover, both studies cited serious flaws in the Pentagon's procedures for spotting sham components.

Whether any of the fakes sold by Aljaff and Felahy went into vital defense systems isn't clear. The Navy declined to comment, saying the case remains under investigation. Nonetheless, recent reports have described several close calls the military has had with bogus chips.

• Because the microprocessors it needed for its F-15 warplanes' flight-control computer were no longer made by the chips' original manufacturer, the military obtained them from a broker, only to discover they were counterfeit, according to the GAO's study in March. Air Force technicians spotted the bad chips before they were installed on the planes' computers.

• That same month, Tobyhanna Army Depot in Pennsylvania discovered it had malfunctioning chips intended for use in military communications systems. "The counterfeit chips failed during testing" and weren't put on any equipment, said depot spokesman Anthony Ricchiazzi.

• In November of last year, a Florida business that makes a device to keep injured pilots from becoming entangled in their parachutes reported finding a counterfeit chip in one of the devices and other fakes in its supply chain. None of the devices were known to have failed, however.

But it's not just the military that's at risk. Chips perform key roles in countless commercial products, as well as phone links, banking networks, electronic grids and nuclear power plants. Given the flood of phony chips, said Diganta Das, a University of Maryland expert on the subject, "we can be assured that we have counterfeit parts in all kinds of systems."

Just ask Billoo Rataul, CEO of Paramit, a contract electronics manufacturing firm in Morgan Hill. Three years ago, his company went to a broker to buy hard-to-find chips and installed them in a Bay Area firm's medical devices. When the equipment began failing at hospitals, he discovered the chips were fakes.

Although the problem was caught before patients were affected, "scores of machines were impacted," said Rataul, who declined to identify the

company and the medical device involved. As a result, Paramit has intensified its efforts to watch for counterfeits because "there is a lot of this stuff floating around."

That was seconded by Don Trenholm, a New Hampshire-based chip-failure analyst. A few months ago, he bought a liquid crystal display for a computer, only to see it suddenly stop working. When he dismantled it to learn why, he found it contained several fake chips.

"It scares me," Trenholm said. "The chance of a counterfeit component showing up on a commercial product is getting better and better."

From November 2007 through May 2010, U.S. Customs officials said they seized 5.6 million bogus chips. Yet many more are finding their way into the U.S. and even the military, which federal officials consider especially worrisome because it could affect national security.

To withstand the rigors of battle, the Defense Department requires the chips it uses to have special features, such as the ability to operate at below freezing temperatures in high-flying planes. And because it pays extra for such chips, experts say, it has become a prime target for counterfeiters.

The Commerce Department turned up 3,868 incidents in 2005 in which the military and its suppliers had encountered counterfeit electronics -- the vast majority of chips -- with each incident potentially involving thousands of phony circuits. By 2008, the most recent data sought, the number had soared to 9,356.

Counterfeiters -- many of them based in China -- often tear apart scrapped computers to obtain chips, which they then mislabel to appear suitable for jobs that exceed the parts' capabilities. That can result in the components suffering dangerous glitches.

Asked whether any military equipment had malfunctioned because of fake chips, Tonya Johnson, a spokeswoman for the Defense Logistics Agency, which buys most of the military's electronic components, said she knew of no such cases. Besides, she said, her agency "has a series of checks and balances in place to block the flow of nonconforming or counterfeit parts from entering the supply chain."

Nonetheless, the Commerce Department study found 14 military organizations, including three with the Defense Logistics Agency, that "reported encountering counterfeit parts in some form."

The recent convictions of Aljaff and Felahy drew praise from the Semiconductor Industry Association, which urged the government to continue cracking down on such offenses, "given the potential for catastrophic injury and damage from failure of a counterfeit microchip." But when it formally commented in March on a federal plan to combat such crimes, the group took issue with the government's enforcement methods.

Customs used to ask legitimate chipmakers to help it check out suspected parts. But it stopped that two years ago, fearing it could be prosecuted for revealing confidential information about the seller of the parts to another company. Since then, the association noted, there has been a "dramatic decrease" in fake-chip seizures. Customs officials told the San Jose Mercury News they are seeking a legal way to once again get help from chip firms.

Other serious roadblocks deter the detection of counterfeits within the military, according to the Commerce Department. It found the armed forces had no reliable method for tracking bogus chips and that numerous attempts to warn military authorities about counterfeits "have fallen on deaf ears."