Bloomberg Businessweek

Magazine

http://www.businessweek.com/stories/2008-10-01/dangerous-fakes

Dangerous Fakes

By Brian Grow,Chi-Chu Tschang,Cliff Edwards andBrian Burnsed October 01, 2008

How counterfeit, defective computer components from China are getting into U.S. warplanes and ships

The American military faces a growing threat of potentially fatal equipment failure—and even foreign espionage—because of counterfeit computer components used in warplanes, ships, and communication networks. Fake microchips flow from unruly bazaars in rural China to dubious kitchen-table brokers in the U.S. and into complex weapons. Senior Pentagon officials publicly play down the danger, but government documents, as well as interviews with insiders, suggest possible connections between phony parts and breakdowns.

In November 2005, a confidential Pentagon-industry program that tracks counterfeits issued an alert that "BAE Systems experienced field failures," meaning military equipment malfunctions, which the large defense contractor traced to fake microchips. Chips are the tiny electronic circuits found in computers and other gear.

The alert from the Government-Industry Data Exchange Program (GIDEP), reviewed by BusinessWeek (MHP), said two batches of chips "were never shipped" by their supposed manufacturer, Maxim Integrated Products in Sunnyvale, Calif. "Maxim considers these parts to be counterfeit," the alert states. (In response to BusinessWeek's questions, BAE said the alert had referred erroneously to field failures. The company denied there were any malfunctions.)

In a separate incident last January, a chip falsely identified as having been made by Xicor, now a unit of Intersil in Milpitas, Calif., was discovered in the flight computer of an F-15 fighter jet at Robins Air Force Base in Warner Robins, Ga. People familiar with the situation say technicians were repairing the F-15 at the time. Special Agent Terry Mosher of the Air Force Office of Special Investigations confirms that the 409th Supply Chain Management Squadron eventually found four counterfeit Xicor chips.

THREAT OF ESPIONAGE

Potentially more alarming than either of the two aircraft episodes are hundreds of counterfeit routers made in China and sold to the Army, Navy, Air Force, and Marines over the past four years. These fakes could facilitate foreign espionage, as well as cause accidents. The U.S. Justice Dept. is prosecuting the operators of an electronics distributor in Texas—and last year obtained guilty pleas from the proprietors of a company in Washington State—for allegedly selling the military dozens of falsely labeled routers, devices that direct data through digital networks. The routers were marked as having been made by the San Jose technology giant Cisco Systems (CSCO).

Referring to the seizure of more than 400 fake routers so far, Melissa E. Hathaway, head of cyber security in the Office of the Director of National Intelligence, says: "Counterfeit products have been linked to the crash of mission-critical networks, and may also contain hidden 'back doors' enabling network security to be bypassed and sensitive data accessed [by hackers, thieves, and spies]." She declines to elaborate. In a 50-page presentation for industry audiences, the FBI concurs that the routers could allow Chinese operatives to "gain access to otherwise secure systems" (page 38).

It's very difficult to determine whether tiny fake parts have contributed to particular plane crashes or missile mishaps, says Robert P. Ernst, who heads research into counterfeit parts for the Naval Air Systems Command's Aging Aircraft Program in Patuxent River, Md. Ernst estimates that as many as 15% of all the spare and replacement microchips the Pentagon buys are counterfeit. As a result, he says, "we are having field failures regularly within our weapon systems—and in almost every weapon system." He declines to provide details but says that, in his opinion, fake parts almost certainly have contributed to serious accidents. When a helicopter goes down in Iraq or Afghanistan, he explains, "we don't always do the root-cause investigation of every component failure."

While anxiety about fake computer components has begun to spread within the Pentagon, top officials have been slow to respond, says Ernst, 48, a civilian engineer for the military for the past 26 years. "I am very frustrated with the leadership's inability to react to this issue." Retired four-star General William G.T. Tuttle Jr., former chief of the Army Materiel Command and now a defense industry consultant, agrees: "What we have is a pollution of the military supply chain."

Much of that pollution emanates from the Chinese hinterlands. BusinessWeek tracked counterfeit military components used in gear made by BAE Systems to traders in Shenzhen, China. The traders typically obtain supplies from recycled-chip emporiums such as the Guiyu Electronics Market outside the city of Shantou in southeastern China. The garbage-strewn streets of Guiyu reek of burning plastic as workers in back rooms and open yards strip chips from old PC circuit boards. The components, typically less than an inch long, are cleaned in the nearby Lianjiang River and then sold from the cramped premises of businesses such as Jinlong Electronics Trade Center.

A sign for Jinlong Electronics advertises in Chinese that it sells "military" circuitry, meaning chips that are more durable than commercial components and able to function at extreme temperatures. But proprietor Lu Weilong admits that his wares are counterfeit. His employees sand off the markings on used commercial chips and relabel them as military. Everyone in Guiyu does this, he says: "The dates [on the chips] are 100% fake, because the products pulled off the computer boards are from the '80s and '90s, [while] customers demand products from after 2000."

BusinessWeek traced the path of components from Guiyu to BAE Systems Electronics & Integrated Solutions in Nashua, N.H. The company's confidential reports to the Government-Industry Data Exchange Program were critical to this research. A unit of BAE's $15 billion U.S. division, the electronics operation makes a variety of sophisticated equipment, ranging from missile-warning systems for fighter jets to laser-targeting devices for snipers. It has reported far more counterfeiting incidents than its rivals: 45 over the past three years. Industry executives say that large figure may reflect BAE's candor or its aggressive pursuit of low-priced chips from China. The Justice Dept. is investigating BAE's military electronic-parts procurement, a company spokesman confirmed.

In a statement, the company said that it "has attempted to pursue the origin of components provided through the supply chain, [but] has no further insight, nor certification to the origins of components that are provided by supply-chain distributors." Only a "small percentage" of its parts have turned out to be counterfeit, BAE said. It now has restricted its purchases to original chipmakers and their

approved distributors "except in very limited circumstances," such as when it needs a hard-to-find component.

BAE isn't unique. Other contractors that have reported counterfeit microchips to GIDEP include Boeing (BA) Satellite Systems, Raytheon (RTN) Missile Systems, Northrop Grumman (NOC) Navigation Systems, and Lockheed Martin Missiles & Fire Control. The companies all said they take the threat of counterfeits seriously but wouldn't comment on specific incidents.

The flood of counterfeit military microelectronics results largely from the Pentagon's need for parts for aging equipment and its long efforts to save money. In the mid-1990s, after the collapse of the Soviet Union, the Clinton Administration launched an initiative, continued during the Bush years, of buying all sorts of components off the shelf. In addition to the traditional pattern of purchasing equipment from original manufacturers and their large, authorized distributors, the Pentagon began doing business with smaller U.S. parts brokers that sprang up to offer low-cost items, including microchips. Federal affirmative-action goals have further encouraged the military to favor suppliers that qualify as "disadvantaged." The chips wholesale for as little as 10 cents and as much as $2,000 each, depending on their complexity and quality. The Pentagon spends about $3.5 billion a year on spare chips, many of them for planes and ships that are 10 or 20 years old.

Name-brand manufacturers and well-established distributors, some of which acquire the rights to make obsolete chips, say they mark up prices 10% to 30%. Smaller brokers settle for far less generous margins. The number of small brokers increased sharply after 1994, when Congress stopped requiring government contractors to certify that they were either original manufacturers or authorized distributors. The brokers have to obtain a contractor code but receive little or no oversight. Hundreds are now operating, some out of suburban basements and second bedrooms. A BusinessWeek analysis of a contracting database identified at least 24 active brokers that list residential homes as their place of business. Several have won chip contracts for "critical applications," which the Pentagon defines as "essential to weapon system performance...or the operating personnel." In many cases these entrepreneurs comb Web sites such as brokerforum.net and netcomponents.com, which connect them with traders in Shenzhen and Guiyu. The brokers sell either directly to Pentagon depots or via suppliers to defense contractors such as BAE.

ON A QUIET STREET

Mariya Hakimuddin owns IT Enterprise, a company she runs with her mother out of a modest one-story house in Bakersfield, Calif. Rosebushes line the street, and a basketball hoop hangs in the driveway. Hakimuddin, who is in her 40s, says she has no college education. She began brokering military chips four years ago, after friends told her about the expanding trade. Since 2004 she has won Pentagon contracts worth a total of $2.7 million, records show. The military has acquired microchips and other parts from IT Enterprise for use in radar on the aircraft carrier USS Ronald Reagan and the antisubmarine combat system of Spruance-class destroyers.

Hakimuddin says she knows little about the parts she has bought and sold. She started her business by signing up on the Internet for a government supplier code. After the Defense Dept. approved her application, with no inspection, she began scanning online military procurement requests. She plugged part codes into Google (GOOG) and found Web sites offering low prices. Then she ordered parts and had them shipped directly to military depots. "I wouldn't know what [the parts] were before I'd order them," she says, standing near her front door. "I didn't even know what the parts were for."

The Navy's Ernst became concerned about IT Enterprise in March 2007. His team found a suspicious transistor—a basic type of microchip—supplied by the firm for use in the AV-8B Harrier, a Marine Corps fighter jet. The transistor, which turned up during an inspection of a military depot in Cherry Point, N.C., was supposed to contain lead in its solder joints, but didn't. That defect could cause solders to crack and the flight control system to fail, Ernst explains. When a member of the team telephoned IT Enterprise in Bakersfield, he heard children chattering in the background, Ernst recalls. "It was the 'Aha!' moment for me on counterfeit parts," he says.

Unknown to Ernst, a separate Defense inquiry later found that at least five shipments from IT Enterprise since 2004 had contained counterfeit microcircuits, including those intended for the USS Ronald Reagan, according to Pentagon records. During her interview with BusinessWeek, Hakimuddin denied any wrongdoing and blamed her suppliers, but she wouldn't name them. In January the Defense Dept. banned IT Enterprise, Hakimuddin, and her mother, Lubaina Nooruddin, from supplying the military for three years.

The Hakimuddins weren't deterred. A month after Mariya was barred, her husband, Mukerram, received his own supplier code, using the same home address with a new company name, Mil Enterprise. This time the Pentagon caught on more quickly, banning Mukerram for three years as well. He couldn't be reached for comment. People familiar with the matter say the Defense Criminal Investigative Service is looking into IT Enterprise.

In written responses to questions about kitchen-table brokers, officials at the Defense Supply Center in Columbus, Ohio—a major Pentagon electronic-parts buyer—said they don't inspect brokers or conduct background checks. "The law does not prohibit" work-at-home brokers or using the Internet to find parts, the officials said. "Is there risk? Yes, there is risk," Brigadier General Patricia E. McQuistion, the center's commander, says in an interview. She estimates that "less than one-quarter of 1% of what we buy is compromised."

RULE CHANGE

Nevertheless, after BusinessWeek's inquiries, the center in August issued new contracting rules for microchips. Suppliers now must document the "conformance" and "traceability" of chips when they place bids. Previously such records didn't have to be filed at the bidding stage and were sometimes missing or faked, industry and government officials say.

Even after the likes of IT Enterprise are identified, it can take time to clean up the mess. On Feb. 5, 2008, a manager at Tobyhanna Army Depot, the Pentagon's largest electronics maintenance facility, in Stroud Township, Pa., notified the supply center in Columbus that his unit had discovered counterfeit chips supplied by IT Enterprise for use in global positioning systems on F-15 fighters, according to internal Pentagon e-mails reviewed by BusinessWeek. The e-mails show that, as late as July, the Columbus center was still trying to locate parts purchased from IT Enterprise.

In a July 24 e-mail, an F-15 engineer, whom BusinessWeek agreed not to identify, wrote: "Suppose that a part like that makes it onto a flight-critical piece of hardware or mission-essential piece of hardware. The[re] is a very good chance that the part may work...but what happens at 40[,000] ft and -50 degrees? Hardware failure. Not good."

Ernst says the Hakimuddin episode helped him realize how blind the military has been: "We don't know how big the counterfeit problem is, and, to me, that is irresponsible." Now he's trying to get others in the bureaucracy to confront what he considers to be a crisis: "The risk of counterfeiting is so

high, and the cost to our weapon systems is so great, that we need to take action." Glenn Benninger, a senior civilian engineer at the Naval Surface Warfare Center in Crane, Ind., concurs: "Counterfeiting has literally exploded over the last few years, but not a lot of people have been paying attention."

The pending investigations could force the Defense Dept. to heed such warnings. In addition to the Justice Dept.'s probe of BAE, there is the Pentagon's in-house criminal inquiry. "The DoD takes this threat very seriously," John J. Young Jr., Defense Under Secretary for Acquisition, Technology, and Logistics, said in a statement. "This security threat will require great vigilance by DoD to defeat, but we will do everything within our power to do so."

Policies aimed at promoting "disadvantaged" businesses have apparently encouraged dealings with brokers that otherwise might seem questionable. Federal affirmative-action goals require the Pentagon to seek to make 22% of its purchases from small contractors—as measured by staff and revenue—including those run by women, military veterans, or members of certain ethnic minority groups. A contracting database refers to IT Enterprise as a "Subcontinent Asian American Owned Business." Hakimuddin wouldn't discuss her ethnicity but says she was born in the U.S.

Daniel Spencer designated his wife, Brenda, as the legal owner of his brokering business, BDS Supply. "I thought we'd get some kind of benefit [from being woman-owned]," says Spencer, 54, who acknowledges that he runs the company with his wife. Working from home in Great Falls, Mont., he says, he buys from legitimate suppliers and has parts shipped to him before sending them on to the Pentagon. But he admits that, despite a background in computers, he doesn't have the expertise to identify fake chips. Promod Dubey, who runs Phoenix Systems Engineering, a broker in Lake Mary, Fla., complains that military procurement offices "want the cheapest possible s--t they can get." Dubey, who lists Phoenix as a "small disadvantaged" business on Pentagon documents, says he acquires parts from China only as a "last resort" because "sometimes the quality is questionable." Neither he nor Spencer has been accused of impropriety in their military work.

Contractor reports to the GIDEP counterfeits database show a total of 115 incidents over the past six years. But "everybody believes the [GIDEP] reports are just the tip of the iceberg," says Brian Hughitt, manager of quality assurance for NASA. Hughitt says that, during testing, NASA inspectors have identified two shipments of counterfeit chips in the past 18 months. One lot was installed in flight hardware. "That's something that is going to be launched into space," Hughitt says, declining to elaborate. "It could have been real bad." NASA, which helps launch military satellites and missiles, is investigating the shipments.

TRACKING THE CONNECTION

To understand the counterfeiting phenomenon, BusinessWeek independently traced four incidents of phony parts that BAE Systems reported to GIDEP. The circuitous trails all led back to China, as did th

---