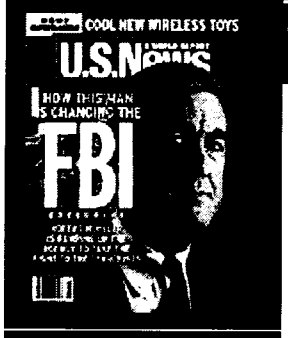

Science & Technology 12/16/02

Crossed signals

The wireless threat to our electronic infrastructure

BY IVAN AMATO

Aboard a commuter jet landing at an Illinois airport in September 2001, a cellphone accidentally left on in an overhead bin caused critical cockpit instruments to go haywire. The air traffic controller instructed the pilots to break off the approach and circle around for a second try. A year earlier, a Boeing 757 on autopilot at 15,000 feet "pitched up rather sharply" in an "uncommanded climb," in the pilot's words. He disengaged the autopilot and leveled out the plane. The cause was never pinned down, but the pilot noted that the plane "acted as if it were under the influence of some electronic glitch or outside influence."

Neither incident, among 50 recorded in the most recent updates of NASA's Aviation Safety Reporting System, ended badly, but they are a cautionary tale for travelers who pooh-pooh flight attendants' requests to turn off electronic devices. They also highlight a growing threat to our microchipped, networked, wireless way of life: electromagnetic interference (EMI), a problem that goes well beyond airplanes.

Think of a hair dryer in the bathroom causing snowy static on the TV in the living room, or a cab driver's radio-carried voice suddenly intruding on your cordless phone conversation. That's electromagnetic interference of a more or less harmless kind. But the growing popularity of wireless links between computers and everything hooked to them is creating more sources of interference, while the wildly successful march of electronics miniaturization is making devices more vulnerable to it.

Spooky. Each isolated case sounds like a fluke: bizarre readings on a

plane navigation system, a car engine-control system that cuts off, an automatic garage door opening for no apparent reason. But together they signal a trend that has convinced some experts that EMI could prove a major technological vulnerability–bad enough if accidental, and potentially far worse if exploited by criminals, terrorists, or military adversaries. "Computers are more susceptible to unintentional and intentional electromagnetic interference than ever before," says Todd Hubing, president of the Electromagnetic Compatibility Society. "With adequate knowledge and resources," he adds, "virtually any electronic system could be disabled, or even destroyed, by electromagnetic interference."

Some experts think it is unlikely to become more than an annoyance. John Pike, head of GlobalSecurity.org, a Washington-area think tank, says, "I worry more about truckloads of fertilizer and suicide bombers." Electromagnetic interference should be easy to tame, he and others say, with simple design changes. But intentional interference may prove hard to defeat, say Hubing and others. Criminals reportedly have begun experimenting with high-powered EMI-based gadgets to defeat computers and alarms. The U.S. military, for its part, has a classified program to develop EMI weapons, which would disarm an enemy by destroying or temporarily scrambling control and communications systems.

For now, the multitudes of electrical and electronic gadgets that fill our lives usually ignore one another, their crisscrossing signals reaching their intended destinations without doing harm. The credit goes in large part to people like Hubing–an unseen army of engineers and regulators acknowledged in the label on almost any electronic device saying, "Tested to comply with FCC standards." Usually, this certifies that the device's electromagnetic emissions–just about any electrical device emits some–will not interfere with licensed radio services, including cellular communications.

But the regulators' efforts may not be able to keep up. The iconic success story of technology–the miniaturization of circuitry–is a major reason. Chips operate at ever faster speeds and lower voltages, making them more vulnerable to interference. On some overpasses in Europe, for example, car engines have suddenly cut off when radio signals generated by high-voltage lines under the roadway interfered with their electronic control units. Certain cellphones, operating at 2.4 gigahertz (billion cycles per second), reportedly go dead near some washing machines because of interference from the machines' motors or electronic controls.

Microwaves–the high-frequency radio signals that are the vehicle for cellphone calls and for the wireless interplay between seemingly every box on sale at Circuit City–are especially troublesome. Their frequencies often match those at which chips operate, and their wavelengths are just right for wending their way into a device. If chips, circuit boards, and other components pick them up like antennas, they can cause digital hiccups. Ones morph into zeros, or vice versa. Erroneous information flows, computers crash, and this time you can't blame Bill Gates.

Burnout. If your neighbor can set off your car alarm accidentally when he orders pizza using his cellphone, the effects of a powerful

microwave beam can be far more dramatic. Computer circuits can burn out entirely, as they did in 1997 in an office building in Germany when circuit boards picked up microwave emissions from a nearby airport's primary radar system. And in March 2001, thousands of drivers in the Bremerton, Wash., area discovered that their keyless locks had stopped working. Suspicions fell on EMI from the warship USS Carl Vinson, which was just arriving in port.

To U.S. military researchers, such incidents point to opportunities and dangers, which have spurred R&D budgeted at nearly $42 million this year. Places like the Air Force Research Laboratory in New Mexico test equipment ranging from aircraft to computers to GPS units to see how vulnerable it is to high-power microwaves, and how it can be protected. Everything seems to matter, including the type of chip, how close internal wires are to an antenna, and the specific microwave wavelengths to which the device is exposed. As one expert put it, move a wire 2 inches and the situation can go from benign to dangerous.

The military has "hardened" its most strategic electronic assets. But the computers in military equipment generally come from the same places that you and I buy ours. And, says James Benford, president of Microwave Sciences Inc. in Lafayette, Calif., and a widely sought EMI consultant, "The PC on your desk is probably the most vulnerable computer in the world right now."

That creates an opening for weapons designers. "A lot of work has been going on in the military area around the world on electromagnetic sources that would be very, very powerful and could harm electronic equipment," says Manuel Wik, a specialist in strategic electronic systems with the Swedish government's Defense Materiel Administration. He has overseen experiments in which a trailer-size system stopped vehicles in their tracks at 1,000 yards by frying their engine-control computers. Similar systems could suppress an incoming missile's navigational electronics. Conversely, a microwave bomb–an explosive device emitting a powerful microwave pulse–could knock out an enemy's air-defense systems. Wik and many others are convinced that EM weapons are going to be a major part of 21st - century warfare.

Pachinko poaching. Also, perhaps, of 21st-century crime. Electromagnetic weapons may have hit the streets already–and not just in the recent movie *Oceans 11*, where an EMI gadget temporarily kills power in Las Vegas. In one case, criminals in Japan's Aichi Prefecture allegedly used a concealed high-energy-radio-frequency device in 1998 to fool a pinball-like pachinko machine into spitting out cash. In another, a thief purportedly used a similar gadget to defeat the alarm system of a jewelry store in St. Petersburg, Russia.

"There are a lot of devices that are quite easily made," says William A. Radasky, president of Metatech Corp. in Goleta, Calif., and cochairman with Wik of a unit recently set up by the International Electrotechnical Commission to study the threats posed by criminal EMI. "It does not take very high energy levels to upset or damage equipment," Radasky notes.

Consider 19-year-old Rostislav Persion, who taught himself skills that

could cause mayhem in the hands of an EMI hacker. While still in high school in Nanuet, N.Y., Slava, as he calls himself, began experimenting in his garage with high-power microwaves. "I actually made my phone lines go dead and my computer too." He admits to once having had "malicious thoughts" but says he is now consumed by the sheer challenge of working with the technology.

Slava buys the components he needs–microwave tubes, banks of capacitors for building up high voltages, and antennas for directing and concentrating the microwave energy–from commercial suppliers and writes his own control software. Now studying engineering at State University of New York-Stony Brook, Slava says he was inspired by David Shriner, a former Defense Department engineer who is now an independent consultant. Shriner, sometimes working under government contract, has been investigating how much damage a person can do on a modest budget by putting together high-power microwave systems from off-the-shelf components.

He and his colleagues have subjected cars, radios, medical intravenous pumps, computers, and other equipment to their homemade, portable gadgetry. The result? Says Shriner: "We have disrupted and destroyed them."

Back to Top