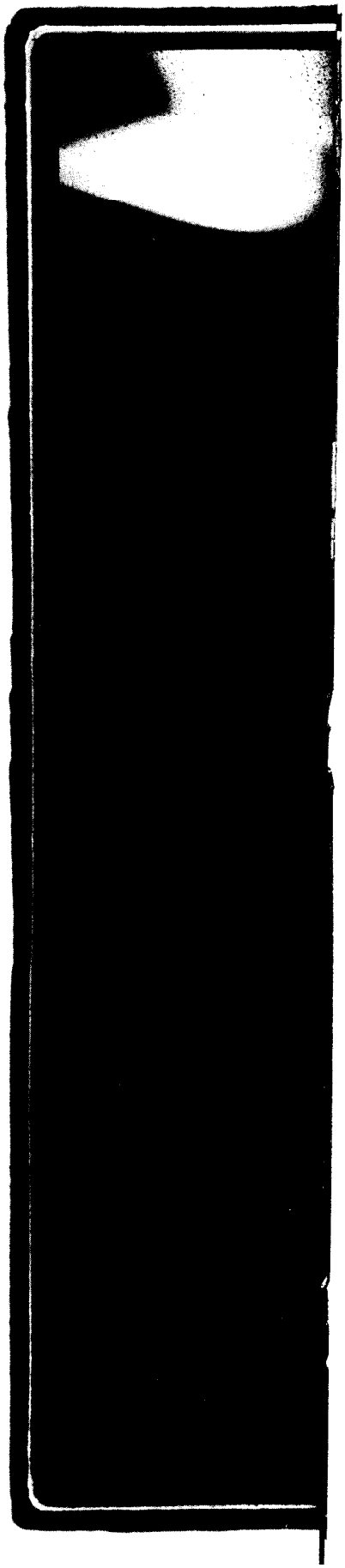
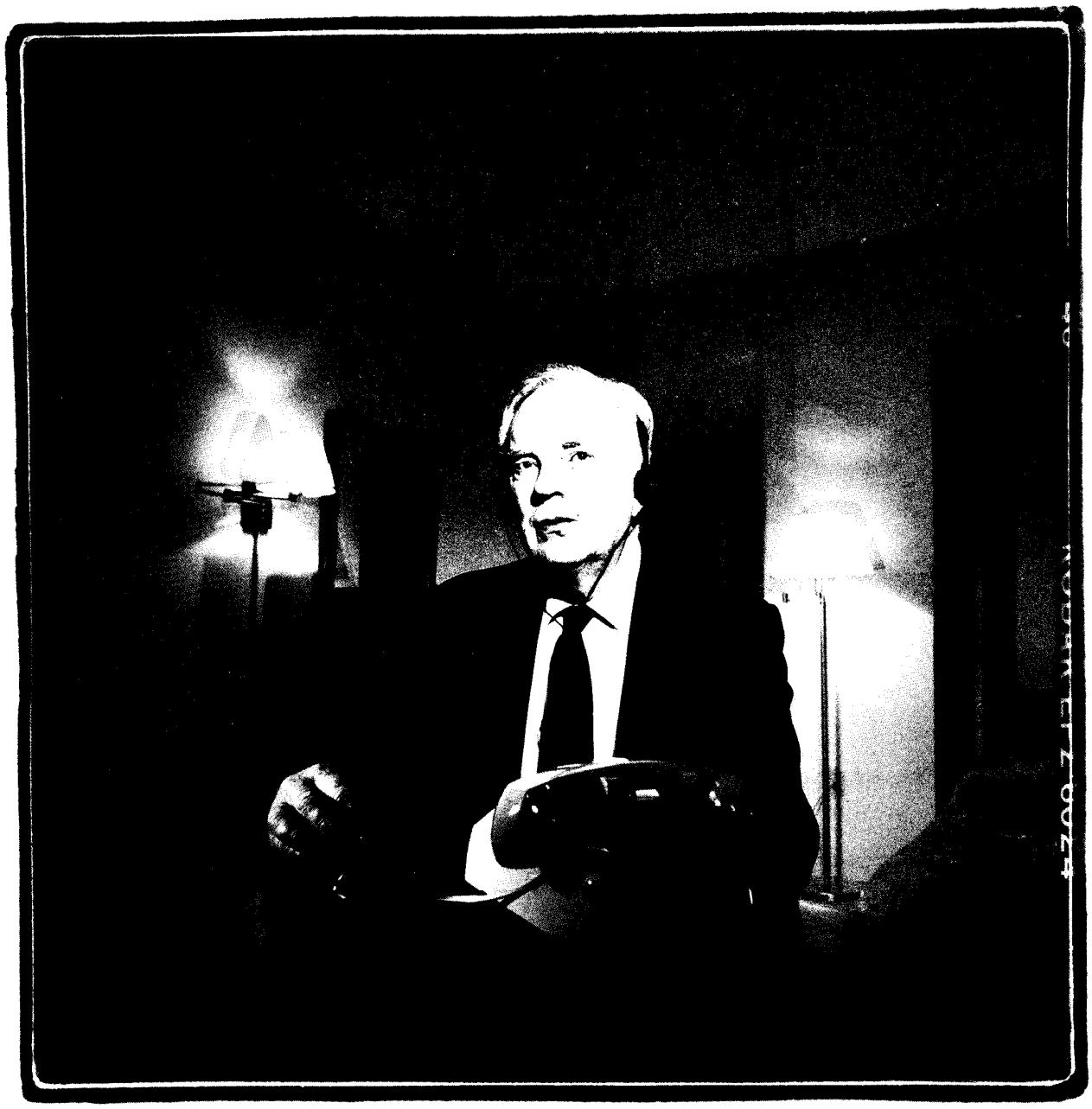
Adventures *in the* Paranoia Trade



Experts in electronic counter-measures live off the fears of corporate clients. But bugging offices may be the least efficient way to spy **By Patrick J. Kiger**

Jim Ross gazed at his spectrum analyzer, beholding what to an electronic countermeasures specialist is a thing of beauty. A small luminous green arc danced across the screen at 75 megahertz. That indicated to Ross that not only were the premises possibly bugged, but that the eavesdroppers might be using a direct-sequence transmitter, a particularly **Photographs by Silvia Otte**



Counter-surveillance pro Jim Ross: the Ross Perot of room sweeps.

sophisticated setup that he'd seen only in demonstrations.

The portly, white-haired ex-Army Signal Corps captain, clad in his usual work garb of a sport shirt and slacks, was a bit overwhelmed. Most of the time, sweeping offices for bugs is like fly-fishing: You make elaborate preparations, pack a lot of gear, practice meticulous technique, and then don't catch anything. But there he was, 3,000 miles away from his home base in Northern Virginia, on the second floor of a legal gambling club in California, and he'd hooked what might have been the biggest fish of his career. We're talking the kind of device that intelligence agencies stick on diplomats' bookshelves, and a system that costs about $40,000. And he was still in the casino boss's office, only a few minutes into his sweep.

"Hey, any chance somebody would've spent that kind of money for a listening system?" Ross asked John Bondi, the casino's security consultant, who'd hired Ross for the sweep job.

Sure, Bondi responded. Compared with what passes through the club every day, that's peanuts. Ross didn't doubt him. On the way in, he'd seen the crowds jammed around the tables, clamoring to play poker and Asian card games even though it was bright and early on a Saturday morning. Business was so good, Ross later learned, that the club feared it might be attracting unwanted scrutiny from government authorities. Not that it mattered to Ross who the hypothetical eavesdroppers might be. It was enough that the client was sufficiently nervous to pay $500 a room to

Surveillance Expo is a sort of World's Fair of paranoia, a key part of Jim Ross's mission to drag countermeasures out of the utility closet and sell them to corporate America.

sweep the premises. In Ross's trade, technical surveillance countermeasures, one man's paranoia is another man's payday.

The president of Ross Engineering is a member of a small, shadowy profession peopled with former cops, retired CIA, Secret Service and FBI agents, and eccentric electronics whizzes. Countermeasures experts earn their living easing the worries of clients who suspect their whispered boardroom conversations may be coming in loud and clear on a tape recorder in a hotel room down the street. They lug around suitcases and steamer trunks full of exotic custom-made contraptions, and speak in a lingo laced with electronics terms and words such as "penetration" and "nullification." They often work nights and weekends, when their probing is less likely to draw attention, and spend long hours poking around in utility closets, perusing the undersides of desks and tables, taking apart public address speakers and testing telephones. Their Holy Grail is the innocuous-looking wire that leads straight to a corporate cabal, the hidden microphone whose discovery will undo a blackmail plot or a sleazy bid rigging attempt by a client's competitor. More often, despite the ominous statistics on industrial espionage and chilling anecdotes in which the trade wraps itself, countermeasures people find nothing. That's why Ross's little arc was cause for excitement.

Just to be safe, though, Ross asked the casino security man to go in the utility closet and flip some breakers. The arc abruptly vanished. Seems that it was being caused by the boss's personal computer.

But before long, Ross picked up another signal—or rather, mysterious little spikes, popping across the screen like fireworks between 275 and 350 MHz. Aha! Seeking to locate the transmission's source, Ross probed the office with his antenna. He dismantled the couch and pulled out the drawers of a half-ton, solid oak desk. Nothing so far. Ross tracked the signal under the desk's right pedestal, where he and Bondi found a telephone jack and a duct going down through the floor. The signal got louder. The source was somewhere beneath them. By now, it was lunchtime, and they weren't even out of the first room.

"Are you sure that's a transmitter?" Bondi asked.

"No," Ross responded, "but it looks like every frequency-hopping transmitter I ever saw." So the search continued. Ross figured that the eavesdroppers might have left an antenna to transmit the signal. He and his helpers carried the bulky, 40-pound analyzer up on the roof, and then took it down to the parking lot and pushed it in a shopping cart around the outside of the building until the analyzer's battery went dead. No luck. The puzzled searchers went back indoors, plugged in an extension cord, and told curious casino employees they were checking for radon as they perused the first floor. While Ross waited outside, Bondi dragged the probe into the ladies' room, directly beneath the boss's office. The tantalizing signal came in strong on the screen.

"Man, you got it!" Ross called out.

"Gentlemen, come inside," Bondi responded. "I want to show you your bug." There on the wall was the source: a small battery-powered air freshener that released both a sweet-smelling aroma and, by sheer chance, a stray electronic signal that looked just like a frequency-hopping bug on the screen. "After that, we checked every other air freshener in the

continued on page 36

Fort Washington debugger Whidden, unlike Ross, prefers to avoid the limelight.

The average company installs a new phone system every five years, leaving in place lots of old wire that provides eavesdroppers with a convenient way to relay conversations.

COUNTERSPIES

continued from page 23

building, but none of them emitted the pulses like that one did," Ross recalls, still shaking his head in disbelief.

Bondi took the air freshener down and sent it to Ross with his paycheck.

THIS ISN'T THE KIND OF STORY YOU would expect to hear told by a countermeasures man, whose fortunes depend on clients' belief that someone really is listening in on their private conversations. Nevertheless, Jim Ross tells it with gusto. In debugging, perhaps the most compulsively secretive cottage industry around, he's a maverick: a guy who loves to talk.

The most conspicuous promoter—and self-promoter—in countermeasures is doing a lot of talking at the fourth annual Surveillance Expo at the McLean Hilton. On this mid-August morning, Ross, the impresario of the four-day exposition, is addressing a group of 30 or 40 people on the subject "Spy Tech: Effective Measures and Countermeasures." He explains some basic surveillance tricks, such as rigging a telephone to transmit nearby conversations even when it's on the hook, as a roomful of dour-faced men in dark suits intently scribble notes. Their lapel tags bear familiar corporate names, such as Apple and Westinghouse, in addition to a host of lesser-known outfits with cryptic techie monikers. Their precise line of business remains obscure, since they tend to stare stonily when a stranger with a notebook walks up and asks them questions.

Ross, however, is receptive to the prospect of media attention. "We're not going to get the whole world to protect themselves," he says. "If you write something that raises the level of paranoia, more power to you."

Indeed, Surveillance Expo is a sort of World's Fair of paranoia, a key part of Ross's mission to drag countermeasures out of the utility closet and sell them as something corporate America should be frightened to do without. It fills the hotel's corridors with an unnerving ambiance that, after a few days, has me looking over my shoulder as I punch my credit card number into pay phones and suppressing the urge to probe the underside of the dinner table for surreptitious matchbook-sized radio transmitters. I've been informed that such devices, though their use is illegal, can be obtained in kit form for a mere $24.95 from mail order companies that dance through loopholes in the federal anti-eavesdropping statute. "Who Knows What Evil Lurks Inside?" proclaims a sign over one vendor's booth. Countermeasures experts offer seminars with titles such as "Penetration of Trusted Systems by Psychological Subversion" and "The Rape of Secure Data Files (How To)."

Early one morning, I squeeze into a crowded lecture hall to hear St. Paul, Minn.-based investigator Kevin Reierson recount the experience of sweeping a hotel suite rented by a law firm for some conferences prior to a big trial several years ago.

"I bumped into the refrigerator, and all of a sudden the modulation on the spectrum analyzer jumped off the screen," Reierson recalls. "It was a place I never would have looked." Just to be thorough, he glanced underneath, where, to his surprise, he found a listening device. "At first, he thought it was a clumsy amateur attempt, since he assumed the hum of the appliance would drown out conversations. Then he checked with the refrigerator manufacturer and learned that the cooling apparatus only needed to run about 20 percent of the time—which meant the eavesdroppers could pick up 80 percent of the conversations.

Later, curious about what it feels like to be spied upon, I contact one of the victims. "Saying that it was a strange feeling is an understatement," Charles Cox III, of the law firm Cox and Goudy, explains to me. "From watching James Bond movies, you know that these things exist. But you don't think it is going to happen to you." Though it's impossible to ascertain what role the ill-gotten information played, Cox's client ended up on the losing side of a multimillion-dollar judgment.

That Reierson not only tells this strange tale but is willing to name a client is a sign of changing times in the debugging biz. Traditionally, it's been a publicity-shy trade; for years its practitioners found gigs through word of mouth or fellow government retirees who'd taken jobs as company security directors. The prototype was Harry Caul, the rigid, humorless protagonist of Francis Coppola's 1974 surveillance epic, "The Conversation," who was pathologically afraid of revealing anything about himself or his work.

That was before the rise of Jim Ross. The 66-year-old Ross, who holds a master's in engineering from the University of Illinois and who dabbled in direct mail advertising and college teaching, discovered in the late 1970s that there was a lucrative living to be made in the corporate counterspying game.

Traditional countermeasure experts looked askance at Ross. "Believe me, there was a lot of resentment of this guy with an education in electronics getting involved in debugging," he explains. "One of the shibboleths that's frequently bandied about is: To be able to find bugs, you must have planted them too. Let's just carry that a step further. We'll not allow any doctor to treat a gunshot wound until he's shot a few people."

He's critical of his competitors: "They know how to pick a lock and get through a door, how to hold a flashlight in their teeth while they're putting something in place." But he says they know nothing about detecting bugs.

Ross has emerged as a stark contrast to Harry Caul. He's the Zig Ziglar of anti-surveillance, the Ross Perot of room sweeps. He touts a survey by Security Management magazine that cites his company as the one most often used and recommended by "corporate decision-

makers" among its readership. He does television interviews, publishes two newsletters for which he claims a combined readership of 17,000, and teaches two-day seminars to would-be debuggers at $750 a head.

If that's not enough, Ross hints at future ventures with pal G. Gordon Liddy, the Expo's keynote speaker, and boasts of another project in the works that he says will virtually eliminate telephone toll fraud.

Promoting the countermeasures trade, though, presents a challenge even for the irrepressible Ross. He is dealing with a murky industry whose members not only lack any formal credentials, but habitually disparage each other as unqualified. Nobody is even sure how many of them there are, though an unpublished survey by Security Management this year cited 20 firms across the country doing business with its corporate readership.

More important, it's tricky to demonstrate how much of a need there really is for countermeasures. There have been a few highly publicized cases of high-tech privacy invasion, such as public airings of the British royal family's sexy phone calls, and the travails of Virginia Gov. Douglas Wilder, who was plagued not only by cellular snoops but by a radio transmitter found in the office of his top aide. News stories have warned us about French spies bugging first-class cabins on Air France flights in their zeal to purloin American manufacturing secrets. And let's not forget the Watergate.

When it comes to serious numbers, though, no one can hazard more than an educated guess about how much illicit electronic surveillance is going on, let alone who might be conducting it. The FBI, normally a font of crime data, thinks so little of the threat that it lumps reports of bugging in with crimes such as cable TV piracy; the last time the bureau broke out the numbers, in 1987, it cited 131 reports, and only 10 percent of those involved snooping for corporate secrets. "Many of the cases that are referred to us are domestic situations, where you have either a husband or wife in a divorce proceeding," says FBI spokesman Bill Carter.

Professional debuggers gripe that law enforcers are blase about electronic surveillance—which is understandable, since cops are doing so much of it themselves (last year state and federal courts approved more than 900 warrants, an all-time high). But even private-sector numbers make non-electronic corporate espionage out to be a far bigger danger. A recent survey of 250 companies by the American Society of Industrial Security reported a 2½-fold increase in business espionage incidents since 1985. Only about 8 percent of those reports—fewer than 50 incidents—involved electronic eavesdropping.

But according to one of that study's authors, Connecticut-based security and debugging consultant Richard Heffernan, his fellow countermeasures mavens can take solace in a crucial caveat: Those are the ones who got caught.

"We felt that because of the difficulty of detecting eavesdropping, this was the tip of the iceberg," says Heffernan. "I'm not from the school that says there is one under every rock. But certainly, with the ease of putting in listening devices or intercepting communications such as faxes and cellular phones, it's clearly a problem. Especially when you're talking about international communications."

VERIFIABLE INSTANCES OF ELECTRONIC snooping are tough to come by. Countermeasures experts cite professional pledges of confidentiality and believe few clients would see much benefit in publicizing how they've been had.

Ross, a gifted raconteur, treats me to a slew of no-name anecdotes: a woman TV reporter whose apartment was bugged, perhaps to catch amorous politicians. The man he caught on videotape removing a battery-powered bug from the ceiling of his boss's office. Unfortunately, there's no way to verify these stories. "I wouldn't even name clients when I was testifying in federal court," Ross responds testily.

Eventually he bends just enough to connect me with John Bondi, the consultant who hired him for the California casino job. He also gives me a six-page single spaced transcript of notes he dictated while doing a sweep of the offices of his most notorious client, Wedtech, in November 1986, shortly before the company sank into a mire of allegations of fraud and political corruption. And he puts me in touch with one other real live former client—retired Christian Science Monitor reporter Bob Hey. Six or seven years ago, Hey recalls, he started noticing odd noises and a loss of volume while talking on the phone in his home in Potomac. By the time he got around to hiring Ross, the noises had stopped. Ross didn't find a bug, though he says he did find a suspicious slice in the outside phone line.

We're not talking inspiration for a new 007 flick here. Which may be why at Surveillance Expo, we hear a lot more about infinitely sexier, unverifiable but nevertheless chilling *potential* menaces lurking out there in the ether. Speaker after speaker outdoes the last in prophesying that the apocalypse of privacy invasion is at hand. Our collective naivete and increasing dependence upon electronic gadgetry, they almost gleefully warn, put us at the mercy of sophisticated spies who, with a little effort, can intercept

In the Cold War, it was easier to use bugs than to cultivate Soviet sources. In America, you can bump into an executive at a cocktail party and he'll tell you every detail of his work.

our faxes, break into our voice mail and capture the radiation emanating from our personal computers so they can print copies of our confidential memos or secret bids on lucrative contracts.

"Nobody pays attention to laws, anyway," explains James Carter, a stocky, bearded Texas-based security expert. "Do you know anybody who drives the speed limit?" He shows me a cellular intercept device that scans the airwaves, spotting and flashing on a notebook computer screen the numbers of hundreds of portable phones in use at that moment in Northern Virginia. "As soon as it locks on a voice channel, you can hear both sides of the conversation," he explains.

The system—for sale to police only—can be programmed to spot the car phones of up to 400 different owners and to tune in when any of them makes a call. "I am trying to make everyone aware that their cellular phone conversations are *not* private," Carter explains. If Carter were up to no good, of course, he'd rewrite his software to capture not just the phone numbers, but also the serial numbers that the phones broadcast so the owners can be billed; he could use them to reprogram other phones and make thousands of dollars worth of long-distance calls at the victims' expense.

Rich Roth, of Bethesda-based Counter Technology Inc., advises his rapt listeners that they aren't necessarily any safer in their offices. The average company now installs a new phone system every five years, leaving in place lots of old wire that provides eavesdroppers with a convenient way to surreptitiously relay conversations. He tells everyone to tighten security inside buildings.

"If the guy has all the time in the world to install this thing," he solemnly warns, "it is going to be very difficult for me to find it." At another panel, though, I am informed that eavesdroppers can avoid having to sneak into offices altogether, since technology exists that allows them to shine a beam at our windows to capture the vibrations our conversations create. (In practice, the latter technology can be thwarted if we simply pull the drapes.) Somehow I do not find this quite as disturbing as the surveillance footage of Howard Stern and Jessica Hahn entering a nightclub, shot for practice by another Expo speaker, an undercover investigator who likes to aim a tiny video camera through a hole in his T-shirt.

JIM ROSS'S HIGH-PROFILE PROMOTIONAL style and brashness—in a recent newsletter, he advocated dismantling a host of federal law enforcement and intelligence agencies—rankle an old-school guy like Glenn Whidden. The ex-CIA specialist describes Ross as "a little bit flaky," and although he doesn't question Ross's technical competence, he thinks the self-styled debugging honcho stoops to conquer. "A lot of the stuff you hear described—I hate to say it—at Surveillance Expo is the pedestrian, run-of-the-mill, private investigator or maybe local law enforcement type of threat," he says. "That show is becoming more and more popular, and it still is way down below what the level of professionalism should be." (When I mention Whidden to Ross, he's quick to say, "Glenn is a nice guy, and technically, I don't think there is anybody with a better radio frequency background.")

Compared with Ross's profile, Whidden's is so low he's almost invisible. When I walk into Whidden's Technical Services Agency in a Fort Washington complex, the bland pastels and travel-poster decor lead me to suspect I've mistakenly wandered into the podiatrist's office or the insurance agency with which he shares the building. Around the corner, though, there's a lab filled with sophisticated equipment, some of Whidden's own invention—he holds five patents—and a computer he uses to design circuitry. The silver-haired 65-year-old wears khakis and a short-sleeved button-down shirt whose pocket is crammed with pens. One might mistake him for a grandfatherly radio repairman, except for the plastic-enclosed medal on his shelf that commemorates his 28-year career in the clandestine services, eavesdropping mostly upon Soviet Bloc officials.

On Whidden's worktable is a phone-tapping device of East German origin. "That old Stasi recorder is out of date," he says, "but I want to know its radiation characteristics." Even now that he's a private sector debugger, old habits die hard. He still goes to old haunts such as Moscow. Instead of planting bugs in government buildings, he sweeps branch offices of multinational companies that are afraid competitors in the new free-market Russia will fall back on old-fashioned police-state methods to gain an edge. On a recent trip there, he managed to ferret out a phone line bug, even though he worried—unnecessarily, as it turned out—that the eavesdroppers might be on to his presence. His host had hired a Russian driver for Whidden, the sort who in the old days informed on tourists for the KGB.

Whidden winces at slip-ups like that, just as he hates it when prospective clients call him on their office phones. "If someone calls and says, 'I think we're being bugged—could you come over and sweep the office? I understand you're pretty good blah blah blah,' they've pretty much queered the deal." These days, he sticks mostly to training and refers routine sweeping jobs to other people, unless the client is willing to practice what he calls "Moscow rules." By this he means a stringent, hush-hush strategy based on the assumption that he's not going up against some guy planting a crib monitor in the ceiling tiles, but an intelligence agency alum turned freelancer like himself. "I'm designing my tradecraft for the sophisticated eavesdropper," Whidden explains.

So far, the only hints such rogue agents might be out there are subtle bits of intelligence Whidden picks up on trips abroad, such as an apparent demand for

certain types of increasingly sophisticated European-made electronics. Nevertheless, he fleshes out these hypothetical adversaries in great detail in his three-volume training manual, which presents a fictional bugging operation called "The Story of Tom, Dick and Harry." A sample: "A tinge of loneliness touched his consciousness, and he began to wonder why he was traveling that way and at that time to take risks that most people would avoid like the plague. He had asked himself the same questions in his former career when he set off on missions, but then, the answer had been easy. It was his duty . . . but now, the work was illegal, and it was the money that guided him. But was it really? Of course not—it was the game!" (Whidden explains the Clancyesque prose by saying: "The security guy is working against a person, not just a black box. Besides, it breaks up the dry technical stuff.")

"The Cold War eavesdropper used good technical tradecraft to protect his penetrations and installations," he says, sounding a bit nostalgic for the days he spent skulking around gray buildings surrounded by fences and mean-looking Soviet or Chinese guards. "To defeat that level of sophistication, you need to employ it on the defensive end." To be on the safe side, Whidden uses counter-counter-counter-surveillance techniques. He likes to show up during regular working hours, when the bugs are most likely to be transmitting, wearing a business suit for cover and packing lightweight gear of his own design that fits into a catalogue case that a salesperson might carry. Rather than combing the building room by room right off, he gingerly works his way in from the outside. A really sophisticated bugger, Whidden contends, would study countermeasures and aggressively thwart them; he might, for example, set up his own analyzer to spot the radiation from the sweeper's equipment, and then turn off the transmitter for his bug whenever the search came close. "That is pretty sophisticated stuff," he concedes, "but it is possible."

IF THE SPOOKS OF WHIDDEN'S IMAGINATION are actually out there, wearing surgical gloves as they place the invoice for their services in plastic bags, we could be in big trouble. There are at least a few advanced bugs—such as a British-made infrared transmitter—that may slip by conventional countermeasures. Contemplate these possibilities long enough and you may end up ripping the plaster off your walls, as Harry Caul did in "The Conversation." At the Surveillance Expo, I try to strike up a conversation with a corporate visitor so discreet that he dispenses with a name tag and doesn't reciprocate when I introduce myself. "You really want to keep something secret?" he asks. "Take the guy out in the parking lot and tell him."

Which brings us to perhaps the dirtiest secret of the countermeasures trade, one on which both Ross and Whidden surprisingly agree: Electronic eavesdropping is not one of the more efficient ways of gathering information.

"If you know when a certain crucial meeting is happening, you can get useful stuff," Whidden says; on the other hand, if an eavesdropper has to sit and listen all day to the sounds in the office, it could be a mind-numbing waste of time.

In the old Cold War days, it was easier to use bugs than to cultivate well-trained, KGB-fearing Soviet bureaucrats as sources. In corporate America, you can bump into an executive at a cocktail party and he'll eagerly tell you every detail of his work.

"If you hired me to get information on XYZ company," Ross explains, "I'd open a phony personnel office and run an ad in the paper." XYZ employees trying to move up to better jobs would be out to impress, and without realizing it would reveal all sorts of confidential data.

In fact, one danger of electronic eavesdropping is that obsession about privacy may prompt people to do really stupid things. Ross recalls a three-day sweep of a Florida company on which he assisted; at one site, he says, "the guy in charge of security is a retired cop. Every day, he patted us down and made us empty our pockets. Chewing gum, combs, everything. I said, 'Tell me what you're looking for, and I'll hand it to you.' After all, I'm carrying all this gear in big cases through the door.

"Anyway, the last day, we went back to the motel where we were staying, and the two guys I was working with started emptying their car trunk. They handed me a briefcase. I said, 'Not mine, must be yours.' They said, 'No, it must be yours.' 'Nope,' I said. It belonged to a manager whose office we just had done. The security guy, trying to be helpful, had picked this thing up and carried it out and put it in the car. We'd just spent the whole bloomin' weekend and they'd spent a lot of money having us protect their secrets. That briefcase contained the entire budget for the year, an analysis of all the projects they had underway, the competition on each one, all the detail. He just handed it to us."

Absentmindedness, it seems, doesn't show up as a squiggly green line on a spectrum analyzer. The more I think about that, it's probably all for the best. ■

Patrick J. Kiger last wrote for the Magazine about business creativity seminars.