Dawn of The E-BOMB

For the wired world, the allure and the danger of high-power microwave weapons are both very real **By Michael Abrams**

In these media-fueled times, when war is a television spectacle and wiping out large numbers of civilians is generally frowned upon, the perfect weapon would literally stop an enemy in his tracks, yet harm neither hide nor hair. Such a weapon might shut down telecommunications networks, disrupt power supplies, and fry an adversary's countless computers and electronic gadgets, yet still leave buildings, bridges, and highways intact. It would strike with precision, in an instant, and leave behind no trace of where it came from.

In fact, it almost certainly is already here, in the form of high-power microwave (HPM) weapons. As their name suggests, HPMs generate an intense "blast" of electromagnetic waves in the microwave frequency band (hundreds of megahertz to tens of gigahertz) that is strong enough to overload electrical circuitry. Most types of matter are transparent to microwaves, but metallic conductors, like those found in metal-oxide semiconductor (MOS), metal-semiconductor, and bipolar devices, strongly absorb them, which in turn heats the material.

An HPM weapon can induce currents large enough to melt circuitry. But even less intense bursts can temporarily disrupt electrical equipment or permanently damage ICs, causing them to fail minutes, days, or even weeks later. People caught in the burst of a microwave weapon would, by contrast, be untouched and might not even know they'd been hit. (There is, however, an effort to build a microwave weapon for controlling crowds; a person subjected to it definitely feels pain and is forced to retreat.)

"HPM sources are maturing, and one day, in the very near future, they will help revolutionize how U.S. soldiers fight wars," says Edl Schamiloglu, a professor of electrical and computer engineering at the University of New Mexico in Albuquerque and one of the leading researchers in this burgeoning field.

The fact that we seldom hear about HPM weapons only adds to their exoticism. Last spring, stories leaked to the press suggested that the Pentagon, after decades of research, had finally deployed such a device in Iraq. And when news footage showed a U.S. bomb destroying an Iraqi TV station, many informed onlookers suspected it was an electromagnetic "e-bomb."

"I saw the detonation, and then I saw the burst—which wasn't much. If they took the station out with that blast, I strongly suspect that we used Iraq as a proving ground" for HPMs, says Howard Seguine, an expert on emerging weapons technology with Decisive Analytics Corp., in Arlington, Va.

But while the U.S. military proudly paraded assorted new war-making technology during its conquest of Iraq, from unmanned combat aerial vehicles to a new satellite-based tracking network, it remained tight-lipped about this "mother of all weapons." Asked at a 5 March news briefing to confirm the rumor, General Tommy Franks, head of U.S. forces during the war, would only say, "I can't talk to you about that because I don't know anything about it."

Military secrecy is nothing new, of course. What is known about microwave weapons is that the U.S. military has actively pursued them since the 1940s, when scientists first

CHIP SIMONS

Microwave weapons researcher Edl Schamiloglu sits in front of the Pulserad-110A accelerator, which his lab at the University of New Mexico uses to produce single 100-nanosecond pulses of electron beams, each pulse emitting hundreds of megawatts of power.

observed the powerful electromagnetic shock wave that accompanied atmospheric nuclear detonations, suggesting a new class of destructiveness. While much of the work on HPMs remains classified, the Pentagon has also recently sponsored a number of U.S. university laboratories to work out the basic principles of microwave weapons, including reliable and compact nonnuclear ways of generating microwave pulses.

Many of those results are being published in the open literature [see To Probe Further, p. 30]. In fact, all you need is a reasonable grasp of physics and electrical engineering to appreciate the ingeniousness of microwave weapons. Anyone with a technical bent could probably also build a crude e-bomb in their garage, a thought that security-minded folks find rather troubling.

How they work

From the military's perspective, HPM weapons, also known as radiofrequency weapons, have many things going for them: their blast travels at the speed of light, they can be fired without any visible emanation, and they are unaffected by gravity or atmospheric conditions. The weapons come in two flavors: ultrawideband and narrowband. Think of the former as a flashbulb, and the latter as a laser; while a flashbulb illuminates across much of the visible spectrum (and into the infrared), a laser sends out a focused beam at a single frequency.

Like the flashbulb, ultrawideband weapons radiate over a broad frequency range, but with a relatively low energy (up to tens of joules per pulse). Their nanoseconds-long burst produces a shock that indiscriminately disrupts or destroys any unshielded electronic components within their reach. The bomb's destructiveness depends on the strength of the ultrawideband source, the altitude at which it is initiated, and its distance from the target [see "E-Bomb Anatomy," p. 29].

Narrowband weapons, by contrast, emit at a single frequency or closely clustered frequencies at very high power (from hundreds up to a thousand kilojoules per pulse), and some can be fired hundreds of times a second, making an almost continuous beam. These pulses can be directed at specific targets—say, a command and control complex positioned on the roof of a hospital in a densely populated neighborhood—and tuned to specific frequencies. Technologically more sophisticated than ultrawideband sources, they are far more difficult to develop, but are reusable and potentially of much greater use to the U.S. military.

Both versions wreak the same kind of havoc on just about any kind of unprotected electronic equipment. Particularly vulnerable is commercial computer equipment; anything in excess of just tens of volts can punch through gates in MOS and metal-semiconductor devices, effectively destroying the device, explains Carlo Kopp, a visiting research fellow in military strategy at the Strategic and Defense Studies Centre in Canberra, Australia, and a computer scientist who lectures at Monash University in Melbourne. The higher the circuitry's density, the more vulnerable it is, because less energy is required to overload and destroy the transistors. HPMs also produce standing waves in electrical grid wiring and telephone and communications wiring, entering through cables, antennas, and even ventilation grills. They can immobilize vehicles with electronic ignition and control systems, too.

"Since the frequency is high, this permits parasitic or stray capacitances to couple energy via paths in the circuit that may not be protected against overvoltage," Kopp explains.

The e-bomb

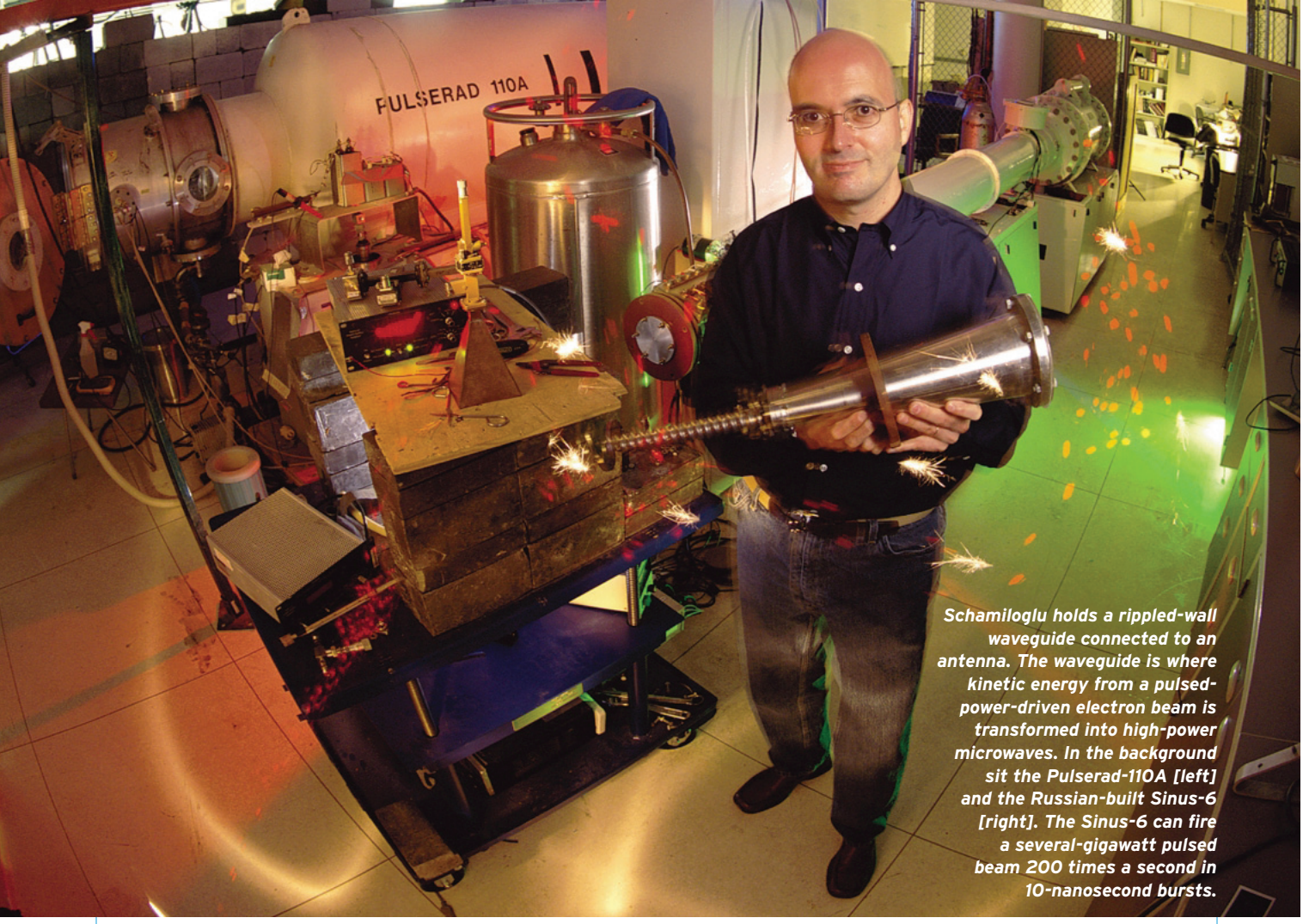
You could deliver an e-bomb in a number of ways: cruise missile, unmanned aerial vehicle, or aerial bomb. Whether ultrawideband or narrowband, the e-bomb consists of both a microwave source and a power source [again, see diagram, p. 29]. Ultrawideband e-bombs aim to create an electromagnetic pulse like that accompanying a nuclear detonation, except that the nuclear material is replaced with a conventional, chemical explosive. The microwave source typically relies on an extremely fast switching device, according to Kopp, who has written widely on weaponizing HPM technology. Narrowband e-bombs might use a virtual cathode oscillator (vircator) tube or a variant of a magnetron. Though termed narrowband, they don't have the high coherency seen in signal-carrying applications, Kopp says.

It takes gigawatts of power to feed an e-bomb's microwave source. For that, the flux compression generator, or FCG, is a good choice, says Kopp. Invented by Clarence ("Max") Fowler at Los Alamos National Laboratory after World War II as a by-product of research into atomic bomb detonators, FCGs are conceptually simple. The best-known type consists of an explosive-packed copper cylinder surrounded by a helical current-carrying coil. Upon detonation, the explosion flares out the cylinder, short-circuiting the coil and progressively reducing the number of turns in the coil, thus compressing the magnetic flux. Large FCGs have produced tens of gigawatts, and they can be cascaded—connected end to end—so that the output from one stage feeds the next.

Despite its simplicity, an FCG-powered e-bomb is probably too difficult for the average terrorist to build on the cheap. For one thing, to test the assembled apparatus, you have to blow it up. For weapons researchers, the e-bomb poses other problems. The strength of the shock wave dissipates rapidly as it moves out from the explosion. To knock out an electrical power substation, for example, the weapon has to strike within about a hundred meters. "Like all microwave radiation, the effect follows an inverse square law with increasing distance," Kopp notes. Though the explosion needed to force out the current can be fairly small, it keeps the munition from being fully nonlethal and nondetectable. Also, anything that's been hardened or shielded against an electromagnetic pulse from a nuclear bomb will probably emerge unscathed.

Focused like a laser

The type of narrowband HPM weapons that the U.S. military is looking at offers everything that e-bombs do not. They're nonlethal, reuseable, and tunable, and they can be fired from miles away. Like a laser, the focused beam disperses only slightly over great distances. With a frequency range that is between about 1 and 10 GHz, they can penetrate even electronics shielded against a nuclear detonation. The deepest bunkers with the thickest concrete walls are not safe from such a beam if they have even a single unprotected wire reaching the surface.



Schamiloglu holds a rippled-wall waveguide connected to an antenna. The waveguide is where kinetic energy from a pulsed-power-driven electron beam is transformed into high-power microwaves. In the background sit the Pulserad-110A [left] and the Russian-built Sinus-6 [right]. The Sinus-6 can fire a several-gigawatt pulsed beam 200 times a second in 10-nanosecond bursts.

CHIP SIMONS

A microwave beam is created much like a laser beam. Between the batteries (or other power source) and the beam sit three elements: capacitors that turn the stored energy into an electron beam of nanosecond bursts, a microwave source that converts the electron beam into focused, high-frequency electromagnetic waves, and an antenna that points and shoots the beam.

Kirtland Air Force Base, in Albuquerque, N.M., is considered the epicenter of the Pentagon's research on pulsed-power electromagnetic weapons. There, its premier pulsed-power system, the Shiva Star, is housed behind meter-thick walls [see photo, p. 28]. An Air Force spokesperson refused to comment on what goes on in their pulsed-power programs, but a fact sheet on the Web site of Kirtland's Directed Energy Directorate describes the Shiva Star as capable of producing "120 thousand volts and 10 million amps for down to one millionth of a second to produce a power flow equivalent to a terawatt."

The Kirtland machine isn't used to investigate HPM weapons per se, and its massive size makes it clearly impractical for delivering microwave beams to any spots of real military interest. Indeed, one big push in microwave weapons has been toward portability. "Back in the 1960s and 1970s, the attitude was, 'Yeah, we can do it—but we need Hoover Dam as our power supply,' " says Seguine. But just as batteries for cellphones and laptops have shrunk and gained capacity, so have sources for microwave weapons.

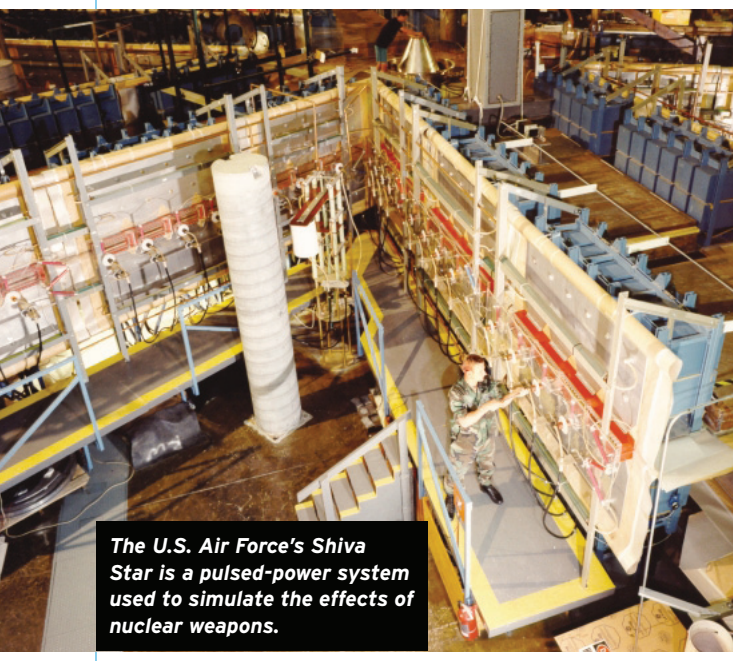
In the 1990s, the U.S. Air Force Office of Scientific Research set up a five-year Multidisciplinary University Research Initiative (MURI) program to explore microwave sources. One of those funded was the University of New Mexico's Schamiloglu, whose lab is located just a few kilometers down the road from where the Shiva Star sits behind tightly locked doors. Thanks in large part to his and his colleagues' efforts, the fundamental capabilities and limitations of high-power microwave sources are now better understood and appreciated.

Amidst the lead bricks and clutter in Schamiloglu's basement lab lies his masterwork: the Sinus-6. "A lot of laboratories come up with very cute names for these devices," Schamiloglu notes with a smile. "We never did." With a huge cylinder at one end connected to the long microwave source, the Sinus-6 looks like a giant torch lying on its side [see photo, above]. The big cylinder contains a Tesla transformer, whose two coils vibrate in resonance and amplify the incoming voltage "with nearly 100-percent efficiency," Schamiloglu says. Once the pulse has been transformed into an electron beam, it is guided by a strong axial magnetic field through the long tube that will turn it into microwaves.

The Sinus-6 can fire a several-gigawatt pulsed beam 200 times a second in 10-nanosecond bursts. "It has to be pulsed power because what you're after is high peak power," says Schamiloglu. "The power in the microwaves is going to depend on the electric field squared, so if you generate very large power, then the electric field is going to be big."

How big? To drive the Sinus-6's beam continuously for an entire second, you'd need to supply about 25 gigajoules—"the entire output of a typical coal-fired electrical plant for 10 full seconds," Schamiloglu says. Another reason for pulsed rather than continuous power is to avoid a problem at the output end: the air around the antenna would heat to a plasma that in turn would interfere with a continuous beam at these power levels.

The key to reaching gigawatts of power is dumping all the energy in one gigantic, nearly instantaneous pulse. A pressurized gas switch prevents the Tesla transformer from prematurely dumping as it builds up for the next pulse. The switch is filled with highly compressed and nonconducting nitrogen gas. When the transformer coils reach 700 kV, the nitrogen gas breaks down, and the pulse leaps through to the electron-beam diode.



The U.S. Air Force's Shiva Star is a pulsed-power system used to simulate the effects of nuclear weapons.

"Once you've fired the switch, it conducts, it generates a pulse," says Schamiloglu. "It conducts because you've made a plasma channel out of the gas. Then you have to wait for that plasma to recombine and form a neutral gas again. A typical time scale for this thing to recombine and fizzle out and be a neutral gas again is probably on the order of milliseconds."

Among the best candidates for supplying microwaves is the backward wave oscillator; it has the advantage of being tunable (plus or minus 20 percent) and producing output in the 4–10-GHz range. To turn the kinetic energy from the Sinus-6's electron beam into high-power microwaves, the oscillator uses a rippled-wall waveguide, also called a slow-wave structure [see photo, p. 27].

The structure sets up standing electromagnetic waves in such a way that energy is rapidly transferred to them from the incoming beam of relativistic electrons from the Sinus-6. This growing energy initially propagates in the opposite direction of the beam's movement—hence the device's name—and is then reflected forward and radiated in the form of high-power microwaves. Backward wave oscillators, by the way, are also being tested as a way to push giant sails into outer space, to detect space debris, and to clear minefields.

Being able to tune an HPM weapon comes in handy when a particular target proves invulnerable to a particular frequency. "Experience has shown that if the frequency is slightly altered, measurable effects are discerned," Schamiloglu notes. People used to believe that varying the frequency of HPMs wasn't practical, but Schamiloglu and his students proved them wrong.

Coincidence and curiosity led to their discovery. Schamiloglu first acquired the Sinus-6 from Russian researchers in the early 1990s. (The Soviet Union once boasted a sophisticated program to develop microwave weapons; after its collapse, parts of that legacy were put up for sale, to the delight of researchers like Schamiloglu.) But once the apparatus was assembled in his New Mexico lab, he couldn't get it to operate as promised, so Russian colleagues flew over to help.

"One of them took the RF structure [the rippled-wall waveguide] and started hammering on the thing," Schamiloglu recalls. When they tried it again, everything worked. "I was baffled why manhandling this RF structure—ramming it in—could affect the power so much," says Schamiloglu. So he started a series of experiments in which he slightly displaced the backward wave oscillator by increments. With a little experimentation assisted by computer simulations, his team found that the frequency could be adjusted by changing the distance between the diode and the microwave source. The result is that the backward wave oscillator is now one of the few pulsed-power HPM sources that can be tuned.

Smaller is better

One disadvantage of this oscillator, however, is that it needs an external magnetic field to create the microwave beam, a major hurdle to making the whole system smaller. The size of the Sinus-6 and attendant equipment in Schamiloglu's basement suggests that the U.S. military is nowhere near fielding a narrowband HPM weapon. "When I first started working on high-power narrowband sources, we joked that you can do more damage dropping this equipment on someone than you can by using it," he recalls. "People know how to make microwave sources in the laboratory. The challenge is to take this and package it into an autonomous platform and have it function at the same parameter levels."

Schamiloglu is now hard at work under a new MURI program to study the possibilities of making a compact pulsed-power source. Current narrowband generators are typically several meters long, batteries not included. Schamiloglu and his colleagues are studying how to incorporate novel ceramics into pulsed-power systems, which they believe will allow the length of such sources to be halved. The trick is identifying materials with a high dielectric constant that can also survive the harsh electric fields. "Materials will be an important part in making the next giant leap," he says.

Life in a glass house

Among those agreeing that narrowband HPM weapons will need more refining before they become truly useful to the military is Loren B. Thompson, chief operating officer of the Lexington Institute, a military think tank based in Arlington, Va. He looked

U.S. AIR FORCE

E-Bomb Anatomy

In this hypothetical design for an e-bomb, a two-stage flux compression generator provides gigawatts of power to the virtual cathode oscillator (vircator), which produces the high-power microwaves. The bomb's destructiveness depends on the microwave source and target's vulnerability to electromagnetic attack, among other things, but a 10-GW, 5-GHz HPM device would have a "lethal" footprint 400 to 500 meters across, producing field strengths of several kilovolts per meter. Such an e-bomb would wreak major havoc if detonated over a heavily populated area.

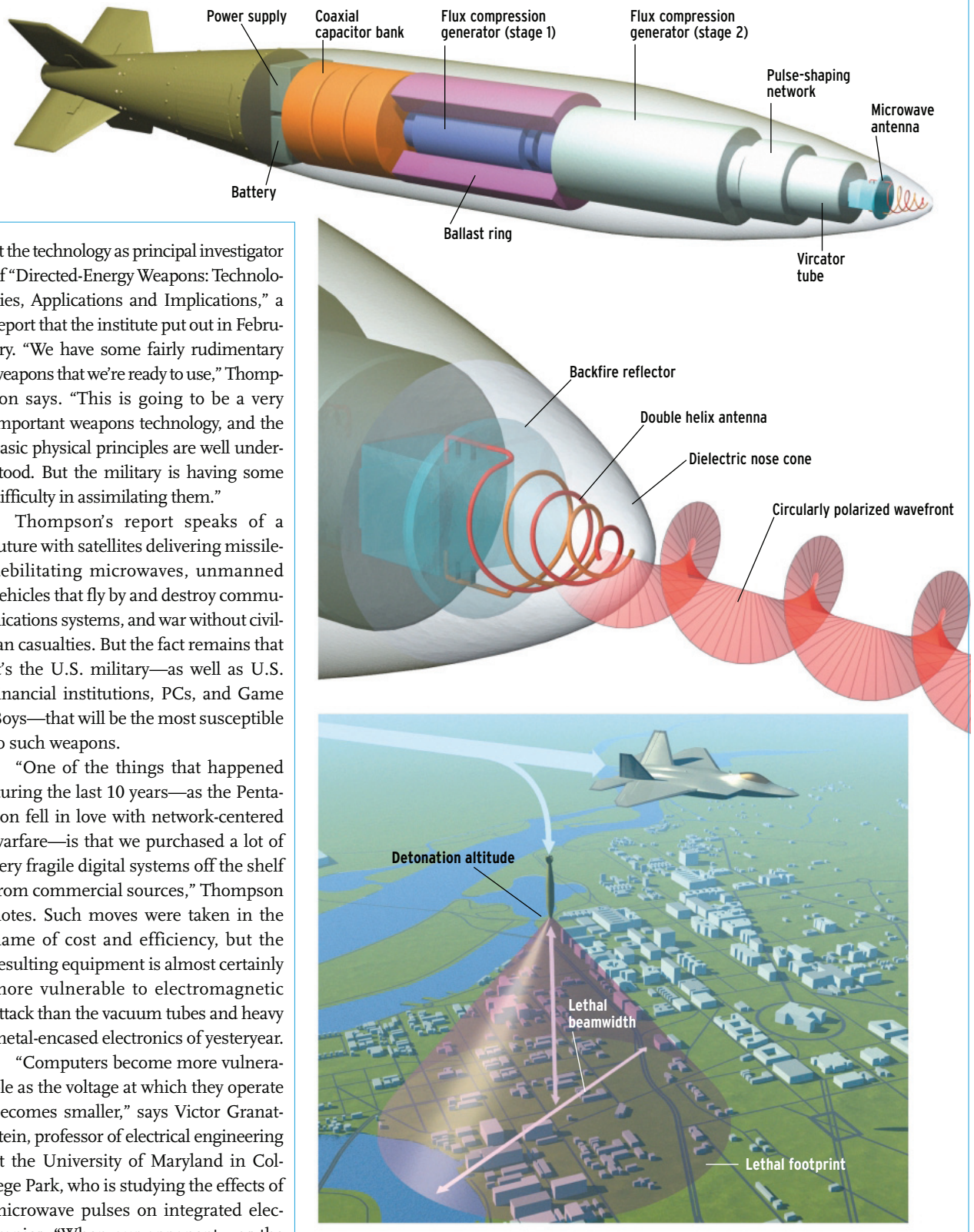


ILLUSTRATION: JOHN MACNEILL SOURCE: CARLO KOPP

at the technology as principal investigator of "Directed-Energy Weapons: Technologies, Applications and Implications," a report that the institute put out in February. "We have some fairly rudimentary weapons that we're ready to use," Thompson says. "This is going to be a very important weapons technology, and the basic physical principles are well understood. But the military is having some difficulty in assimilating them."

Thompson's report speaks of a future with satellites delivering missile-debilitating microwaves, unmanned vehicles that fly by and destroy communications systems, and war without civilian casualties. But the fact remains that it's the U.S. military—as well as U.S. financial institutions, PCs, and Game Boys—that will be the most susceptible to such weapons.

"One of the things that happened during the last 10 years—as the Pentagon fell in love with network-centered warfare—is that we purchased a lot of very fragile digital systems off the shelf from commercial sources," Thompson notes. Such moves were taken in the name of cost and efficiency, but the resulting equipment is almost certainly more vulnerable to electromagnetic attack than the vacuum tubes and heavy metal-encased electronics of yesteryear.

"Computers become more vulnerable as the voltage at which they operate becomes smaller," says Victor Granatstein, professor of electrical engineering at the University of Maryland in College Park, who is studying the effects of microwave pulses on integrated electronics. "When our opponent was the

Soviet Union, the electronics were much more robust because they weren't miniaturized. Now they have very thin oxide layers that can easily break down." Wireless networking makes matters worse. Computers and other communications devices now have antennas attached, giving an electromagnetic pulse a direct pathway to its guts.

Meanwhile, the U.S. Navy no longer requires that all its hardware be hardened against nuclear electromagnetic pulses. It deemed that maintaining those standards was too costly and slowed down the integration of new technology. The presumption was that after the Cold War, nobody would be using nuclear bombs, says the Lexington Institute's Thompson. "Whenever I ask the admirals, 'Well, what if someone did use a nuclear bomb?,' I just get this kind of blank I-don't-have-an-answer-for-that sort of look."

Don't Try This at Home

First things first: we do not under any circumstances recommend that you build your own electromagnetic weapon. But if you're hellbent on adding to the mayhem, cheaply and without too much studying, you might try a high-energy radiofrequency, or HERF, gun. As described by engineering student Rostislav Persion on his Web site, Voltage Labs, which is devoted to do-it-yourself electromagnetic weapons, you can make one from a microwave oven.

Before you begin, though, wait until everyone else has left the house. Next, take apart the microwave oven, but don't disconnect any of the components; manufacturers intentionally make this hard to do, so you may end up just breaking the machine. Inside you will find the oven's microwave source: the magnetron. Wrap a tube of sheet metal around it to act as a waveguide. Your power source is the house's ac, so just plug in the oven and point it at your TV. Warning: there's a real possibility that you will burn yourself instead.

For schematics and a demonstration, head to the Web at http://www.voltsamps.com/pages/projects/herf004/. —*M.A.*

In the wrong hands

The scariest part of microwave weapons may be that crude forms of the technology are readily available to anyone right now. "Any nation with a 1950s technology base capable of designing and building nuclear weapons and radars" can build an e-bomb, says military analyst Kopp. Indeed, more than 20 countries now have programs to develop some type of RF weapon.

"The more widespread the technology is, the more likely that people with nefarious purposes will have access. It's just an inescapable fact," says Thompson. "I don't know what we're going to do. Nobody in Washington knows. I imagine that the way the clear thinking starts is with a catastrophe."

Criminals and pranksters have already started exploiting that weakness. In one of the more harmless applications, a Japanese scam artist rigged up a weak microwave generator inside a suitcase to rip off a pachinko parlor. When he placed the suitcase next to one of the machines (which is something like a cross between a slot machine and a pinball machine) and turned it on, the pachinko machine went haywire and disgorged a pile of coins. The perp managed the trick several times before he was caught.

Other press accounts hint at electromagnetic weapons being deployed by Chechen troops, and by an unnamed assailant trying to topple London's futures market [see "Don't Try This at Home," above].

Thankfully, protecting yourself against the microwave-enabled goofballs of the world isn't too difficult. "It is analogous to existing techniques used to trap RF interference inside equipment, except that the higher power levels require special measures," Kopp notes. Rooms or equipment chassis must become electrically sealed Faraday cages, and protective devices must be added wherever cables enter the protected volume. "Optical fibers are very useful in this game."

Such protective measures are a lot cheaper to design in from the beginning than to add on afterward, says Howard Seguine. "The general rule of thumb is that if you do the hardening during the design phase, it increases the cost roughly 1 percent. If you do it afterward, it may cost as much as 30 percent more."

But maybe hardening is a waste of time. Arthur Varanelli, a Raytheon Co. engineer who has helped write several IEEE standards for electromagnetic field measurement, human exposure, and safety, is skeptical that a malicious prankster could exploit the technology.

"Some of this stuff is just so far out there," Varanelli says. "I just don't see people running around with Buck Rogers ray guns. It's great for a science fiction writer, great to prey upon people's fears." He scoffs at the suggestion that a do-it-yourselfer could build a microwave weapon potent enough to do real damage. "People can put tacks in the road. Are we worried about electronic tacks in the air?"

The wide disparity in opinions and the uncertainty about microwave weapons, from Loren Thompson on one end to Arthur Varanelli on the other, are all part of what makes them so powerful, says military analyst John Pike, who is director of GlobalSecurity.org (Alexandria, Va.). "It all depends on the complex interactions between the weapon and the target," he notes. "I can set up a strap-down chicken test that makes [an HPM weapon] look pretty good. But as soon as I start getting into real-world targets, maybe it doesn't work so well."

"Part of the story is we don't know what the story is," Pike says. "These are weapons that by their nature seek the shadows. And unlike cluster bombs or atomic bombs, they aren't going to leave behind unambiguous evidence of their use." ●

To Probe Further

For a detailed technical discussion of high-power microwaves, see *High-Power Microwave Sources and Technologies*, edited by IEEE Fellows Robert J. Barker and Edl Schamiloglu (Wiley–IEEE Press, 2001). Schamiloglu is also coauthor, with James Benford and John Swegle, of the forthcoming *High-Power Microwaves*, 2nd edition (Institute of Physics, 2004).

The truly prepared, or merely paranoid, will want to consult Carlo Kopp's "Hardening Your Computing Assets" at http://www.globalsecurity.org/military/library/report/1997/harden.pdf.