Fear of Frying

Electro-magnetic weapons threaten our data networks. Here's how to stop them

By **WILLIAM A. RADASKY**

Photography by **DAN SAELINGER**


03:59:07

In the 2001 action movie *Ocean's Eleven*,

criminals use an electromagnetic weapon to black out a portion of Las Vegas. Very futuristic, you may say, but the threat is real and growing.

The problem is growing because the technology available to attackers has improved even as the technology being attacked has become more vulnerable. Our infrastructure increasingly depends on closely integrated, high-speed electronic systems operating at low internal voltages. That means they can be laid low by short, sharp pulses high in voltage but low in energy—output that can now be generated by a machine the size of a suitcase, batteries included.

Electromagnetic (EM) attacks are not only possible—they are happening. One may be under way as you read this. Even so, you would probably never hear of it: These stories are typically hushed up, for the sake of security or the victims' reputation. Occasionally, though, an incident comes to light.

In May 2012, for instance, the *Korea Herald* reported that over 500 aircraft flying in and out of South Korea's Incheon and Gimpo airports reported GPS failures, as did hundreds of ships and fishing boats in the sea west of Incheon Airport. The source of the EM fields was traced to the North Korean city of Kaesong, about 50 kilometers north of Incheon. South Korean officials indicated that North Korea had imported truck-based jamming systems in 2010 that had the capability to jam GPS signals. These officials speculated that one purpose of the jamming was to interfere with South Korea's highly digital society. Or perhaps the North Koreans were conducting an experiment, using South Korea as their beta tester.

In decades past, the few key electronic systems that existed worked at higher voltages than today's machines and at lower frequencies, making them less sensitive to EM disruption. Today, though, any digitally controlled infrastructure presents a target: Power, telecommunications, finance, water, natural gas, and more are all coming under the ever-finer control of computers. Right now the power systems in developed areas of the world are installing smart power meters in homes and businesses, along with communications systems to transmit the data. The new wave of distributed renewable power systems requires additional sensors to determine their operating status, so that the grid can operate efficiently and avoid collapse. The increased need for information and the means to communicate it make all these systems vulnerable to anyone who may wish to create problems—and that means hackers, criminals, vandals, and terrorists.

And, unlike other means of attack, EM weapons can be used without much risk. A terrorist gang can be caught at the gates, and a hacker may raise alarms while attempting to slip through the firewalls, but an EM attacker can try and try again, and no one will notice until computer systems begin to fail (and even then the victims may still not know why).

Governments and professional organizations have been aware of the problem (called intentional electromagnetic interference, or IEMI) at least since the 1990s; in the wake of attacks like the one in South Korea, they began to take it seriously. For instance, in 2012 the European Union began funding three projects to deal with assessing EM attacks and protecting critical infrastructures from them. One project, known as Secret (Security of Railways against Electromagnetic Attacks), is meant to find ways to prevent the jamming of railroad equipment that uses the new GSM-Railway wireless communication standard. It's not enough to patch holes that bad actors have discovered; we must also try to anticipate attacks that haven't yet occurred. It may seem strange that we should find ourselves in need of defending against electromagnetic generators, a kind of weapon most people have still never heard of. The reason is obvious: Not only is it getting easier to make these generators, but we are also becoming more dependent on the data networks those generators threaten.

The recipe for frying a network is simple. Begin with a generator, fold in a battery, and garnish with either an antenna to propagate the output or a hardwired connection into the building you have targeted. Even a briefcase-size model could generate EM fields with peaks in the thousands of volts per meter, and those peaks would come fast and short, with a rise time of about 100 picoseconds and

PREVIOUS PAGE, CGI: SWELL; PREVIOUS PAGE AND THIS PAGE, PROP STYLIST: BIRTE VON KAMPEN

a pulse width of about 1 nanosecond. Such a pulse would contain frequencies between 100 megahertz and several gigahertz.

Whether the attacker transmits via an antenna or a hardwired connection depends on circumstances. The radiated field method gives attackers greater flexibility, but the power decreases rapidly the farther they are from the target. A hardwired approach lets attackers put the pulsed power where they want it without as much wastage, but it does require that they get close enough to the target to make the physical connection. Even this needn't be very hard: Many commercial buildings have vulnerable communications cabinets and external power outlets, as Daniel Månsson, at the KTH Royal Institute of Technology, in Stockholm, has documented.

An attack might be staged as follows. A larger electromagnetic weapon could be hidden in a small van with side panels made of fiberglass, which is transparent to EM radiation. If the van is parked about 5 to 10 meters away from the target, the EM fields propagating to the wall of the building can be very high. If, as is usually the case, the walls are mere masonry, without metal shielding, the fields will attenuate only slightly. You can tell just how well shielded a building is by a simple test: If your cellphone works well when you're inside, then you are probably wide open to attack.

When the pulsed fields enter the building, they induce a current in the internal wiring that flows into the electronics, either damaging the equipment or just producing a disruption, which in turn might require a manual restart or corrupt some data.

The fields are of two kinds: narrowband and wideband. A narrowband waveform is essentially a single frequency of power, delivered over a period of anywhere from 100 ns to several microseconds. Narrowband attacks are usually of very high power, on the order of thousands of volts per meter. Achieving such strong fields is fairly easy because the electrical energy is concentrated in a narrow band. The frequency can be optimized for one purpose and then modulated for another. For instance, the attackers might beam in a gigahertz wave—perfect for penetrating small apertures in equipment cases—and then modulate it to produce a lower-frequency signal (just as AM radio is modulated to encode music). That lower-frequency signal, in turn, is intended to pour energy into the electronics inside the case. But the attack will succeed only if the frequency matches the resonance pattern in the equipment. If no resonance occurs, or if the resonance is confined to just a portion of the equipment, then the effect will be much less serious, or nonexistent. To increase the odds that such "coupling" occurs, the attacker can continue to shift the signal to other frequencies.

Wideband (sometimes called ultrawideband) packs a different punch. Here, the power of each pulse is spread over a range of frequencies, for example, from 100 MHz to 1 gigahertz. If the range is wide enough—that is, if the ratio of the highest to the lowest frequencies in a single pulse is 10 or more—it's considered hyperband. There's less power at any one frequency, and that means less damage will be inflicted per pulse than in a narrowband attack. But wideband pulse generators can easily produce 1,000 pulses per second for many minutes at a time, and that greatly increases the chance of damaging a system, or at least interfering with communications through a straightforward denial of service. Yury Parfenov, of the Russian Academy of Sciences, Joint Institute for High Temperatures, has demonstrated how a high repetition rate can reduce wired Ethernet communications to nearly zero.

And because each pulse requires minimal energy to generate, the energy supply for such a weapon is modest compared to what a narrowband weapon requires. In our laboratory at Metatech Corp., an EM consultancy in Goleta, Calif., we have built a power supply from an automobile battery and an inverter, and it can operate our wideband pulser for days without losing its charge.

Over the past 15 years, our laboratory and others in Germany, Norway, Russia, Sweden, and the United Kingdom have conducted hundreds of experiments studying how commercial equipment holds up to both narrowband and wideband attacks. The emphasis has been on personal computers, alone and in networks, but more recent testing has included cash machines, industrial control equipment, substation electronics, power supplies, Ethernet components, Wi-Fi networks, automobiles, GPS electronics, cellular phones, tablets, and various sensors.

Computers and other systems based on microprocessors turn out to be vulnerable to radiated narrowband fields above 30 volts per meter, although newer high-speed PCs appear to be resistant up to about 300 V/m at some frequencies. That's largely because U.S. and European rules now limit the amount of EM radiation that such machines can emit to the 1- to 10-GHz range, and those rules have had the effect of increasing the machines' shielding. What's more, as the frequency rises from 1 to 10 GHz, computers become less vulnerable to narrowband attack, according to experiments by Richard Hoad at QinetiQ Group, a defense technology company in England. That's good news, but remember, not all industrial computers use high-speed processors. Slower microprocessors (present in programmable logic controllers, for example) don't emit in the gigahertz range, and so they are not well protected against EM attacks in that same frequency range.

In other experiments, Hoad has determined that the presence of metal connecting cables typically increases the vulnerability of the computer equipment. Attacking and damaging small handheld equipment that has no connected cables, by contrast, requires very high fields, usually with peaks greater than 5 kilovolts per meter.

Cables also weaken the defenses of industrial and power-system controls, as shown by Edward Savage, my colleague at Metatech. He simulated attacks, then found that a disproportionate number of equipment failures had originated in cable interface cards. This work suggests that for hooking together the nodes of a network, fiber-optic cable (without metal components) is definitely preferable to copper cable.

Other researchers around the world have determined which kinds of wideband pulses are most dangerous to which kinds of equipment. For instance, a peak electric field of about 2 kV/m for pulse widths on the order of 200 ps can disrupt

The Walls Have Eyes

To make sure your company's electronics aren't wide open to attack, follow these simple rules of electromagnetic hygiene

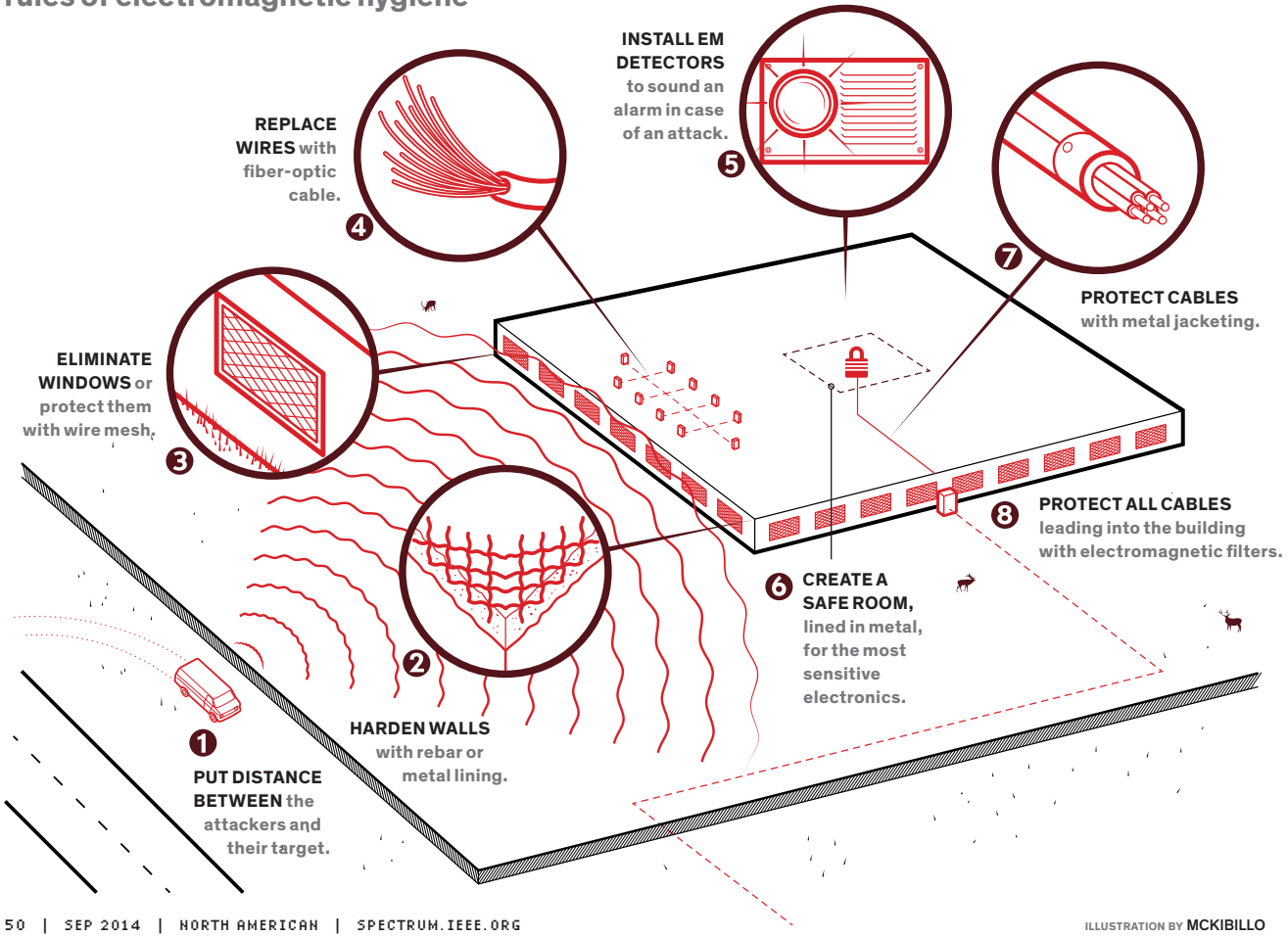
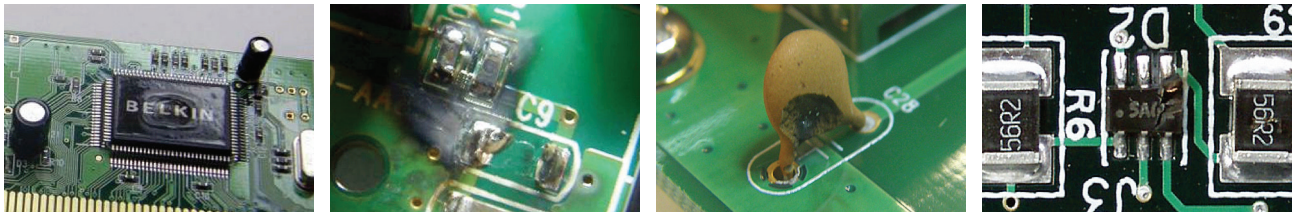


ILLUSTRATION BY MCKIBILLO



CIRCUITS FLAMBÉ, with crisped chips and broiled boards, resulted from tests with pulsed electromagnetic radiation in the author's laboratory at Metatech Corp., in Goleta, Calif. The damage, from left, is as follows: A lid of an integrated circuit was scorched and warped; the capacitor labeled "C9" was completely blown away; part of a ceramic capacitor was shorn off; and the right-hand edge of a small integrated circuit was blasted.

microprocessor-based systems enough to force administrators to push the reset button (although resets do not always work and sometimes the operating system must be reloaded). Peaks at around 5 kV/m will fry the chips beyond redemption.

In these experiments, the field strengths were determined by placing the targeted equipment within the line of sight of a radiating antenna. Of course, if the way is blocked by windowless walls, particularly walls that contain metals, the fields will be attenuated and any damage or disruption will be diminished, if not prevented.

Our electronics are vulnerable for a simple reason: They were designed to handle naturally occurring electromagnetic radiation, but not the malicious sort. By design, they resist narrowband electric fields below 10 V/m for frequencies above 80 MHz; if they didn't, they'd suffer interference from any passing mobile phone or walkie-talkie, and you'd have trouble operating your PC whenever you received a phone call on your handset. Today's electronic products can also withstand a certain level of electrostatic discharge; otherwise, the gentlest spark from a finger on a dry winter's day would be enough to scramble a computer's brains. Electrical and communication cables also have a certain amount of built-in electromagnetic immunity.

The typical specification (such as the standard IEC 61000-6-1) requires that your home computer, for instance, must survive a 1-kV pulse in the cable—a pulse that can itself be induced by a transient EM field of 1 kV/m. Greater protection is typically required in special cases, such as in a power-generating facility or substation. The usual test for electromagnetic immunity involves waveforms with rise times as fast as 5 ns and pulse widths as long as 700 ms—far less threatening than the faster pulse rates that attackers are capable of sending.

Take the Jolt simulator, an experimental wideband generator developed by the U.S. Air Force (and described in the *Proceedings of the IEEE* in July 2004). It produced an electric field of 50 kV/m from 100 meters away, inducing voltages of 50 kV on short cables. That's more than 10 times what it takes to wreck most unprotected electronics!

Obviously, the mandated immunity levels of commercial electronics are too low to protect against EM weapons. We must take steps to harden them, especially the electronics that control our critical infrastructures.

The first line of defense should be putting as much distance as possible between you and the attacker. For instance, you could surround a building with a broad green meadow protected by fences, thus taking advantage of the falloff in an antenna's electric field strength with distance. That's not always possible, of course, so at the very least, you should locate critical equipment away from the building's outermost walls.

The second line of defense involves the building in which the sensitive electronics are housed. No cable should enter the building without first passing through a specially designed surge arrester and a filter protection device coupled to a low-inductance grounding system. The surge arrester will "clip" a high-voltage pulse, but it will also generate some additional high-frequency noise, which the filter protection device will remove. The third line of defense lies in the walls themselves. Ideally, they should contain no windows, which are rather transparent to high-frequency EM fields; if there must be windows, cover them with metal screens. You should harden the walls with metal, such as concrete reinforced with rebar or even metallic wallboard. Best of all is a complete metal shield.

If you can't seal the entire building, you might instead consolidate critical equipment into a room with a solid metallic wall or a specially designed metal screen. Call this the fourth line of defense. Hospitals already use such "screens" to shield powerful MRI machines; here the purpose is not to keep electromagnetic radiation out but to keep it in (so that it doesn't damage computer systems in other rooms).

Finally, you can try to limit the damage should an attack occur. To reduce the coupling of the fields to the cables and equipment, for instance, you can lay the cables along metallic surfaces, cover the cables and connectors with shielding, and install surge protectors at the connection of the cables to each piece of electronic equipment. Even better: Connect these nodes with optical cable rather than metallic wire.

Another obvious way to limit the damage once an EM attack is under way is to shut things down fast. To do that, you need an EM detector to sound the alarm. That's more difficult than it may seem because it requires a detector that can handle all possible attacks, from narrowband to hyperband. Researchers at QinetiQ have built and tested prototype detectors that are good up to 8 GHz, but it will be some time before these products reach the market. Still, even an imperfect alarm would be welcome. Even if it can't mitigate an attack, the information it records could later help forensic analysts to reconstruct the course of events.

Research on cost-effective defenses against EM attack goes on, notably through the International Electrotechnical Commission, in Geneva, the IEEE's Electromagnetic Compatibility Society, and Cigré, in Paris, which studies the reliability of high-voltage power grids. Meanwhile, the operators of threatened facilities must make the best use of the methods that are now available. It's the job of the engineering community to bring those methods to light. ■

POST YOUR COMMENTS at http://spectrum.ieee.org/emattacks0914

METATECH CORP. (4)