Future Tense, one of the revolving features on this page, presents stories and essays from the intersection of computational science and technological speculation, their boundaries limited only by our ability to imagine what will and could be.

DOI:10.1145/1897852.1897879

Gregory Benford

Future Tense
Catch Me If You Can

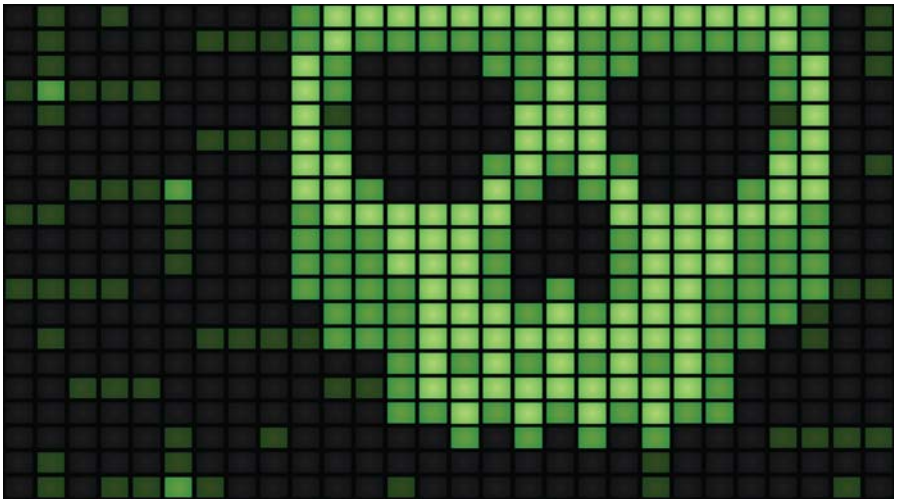
Or how to lose a billion in your spare time...

I ENVISIONED AND wrote the first computer virus in 1969 but failed to see that viruses would become widespread. Technologies don't always evolve as we'd like. I learned this then but failed to catch the train I knew, even then, would soon leave the station. Further, I failed to see the levels of mistrust that would derive from malware generally. I also did not anticipate that seeds of mistrust could be blown by the gales of national rivalry through an Internet that would someday infiltrate every aspect of our lives.

At the Lawrence Radiation Laboratory I used the Advanced Research Projects Administration's network, or ARPANet, to send brief messages to colleagues in other labs running over the big, central computers we worshipped then. However, ARPANet email had a potentially pernicious problem—"bad code" that could arise when researchers sent something new (maybe accidentally), possibly sending yet other things awry.

One day I thought maybe I could add such code intentionally, making a program that would copy itself deliberately. The biological analogy was obvious; evolution would favor it, especially if designed to use clever methods to hide itself and tap other programs' energy (computing time) to further its own genetic ends.

So I wrote some simple code and sent it along in my next ARPANet transmission. Just a few lines in Fortran told the computer to attach them to programs being transmitted to a particular terminal. Soon it popped up in other programs and began propagating. By the next day it was in a lot of otherwise unrelated code, so I wrote a memo, emphasizing to the mavens of the Main Computer that what I had done could likewise be done with considerably more malevolent intent. Moreover, viruses could move.



I avoided "credit" for the idea for a long time but gradually realized the virus-infection metaphor was inevitable, fairly obvious in fact. In the early 1970s it surfaced again at Livermore when a self-replicating program called Creeper infected ARPANet, just printing on a user's video screen "I'm the creeper, catch me if you can!" In response, users quickly wrote the first antivirus program, called Reaper, to erase Creeper. Various people reinvented the idea into the 1980s, when a virus called Elk Cloner infected early Apple computers. It was fixed quickly, but Microsoft software proved more vulnerable, and in 1986 a virus called Brain started booting up with Microsoft's disk operating system and spread through floppy disks, stimulating creation of the antivirus industry I had anticipated in 1970.

It is some solace, I suppose, that the 2010 second-best-selling virus-protection software was a neat little package called Vaccine. The same basic idea was adapted into a different kind of currency in the hands of renowned British biologist Richard Dawkins, coining the term "memes" to describe cultural notions that catch on and propagate through human cultural mechanisms. Ranging from pop songs we can't get out of our heads all the way up to the Catholic Church, memes express how cultural evolution occurs so quickly, as old memes give way to voracious new ones.

Nowadays there are nasty scrub-everything viruses of robust ability and myriad variations: Trojan horses, chameleons (acts friendly, turns nasty), software bombs (self-detonating agents, destroying without cloning themselves), logic bombs (go off given specific cues), time bombs (keyed by clock time), [CONTINUED ON P. 111]

ILLUSTRATION BY JOHN DAVID BIGL III

[CONTINUED FROM P. 112] replicators ("rabbits" clone until they fill all memory), worms (traveling through networked computer systems, laying eggs), and plenty more.

Viruses were not a legacy I sought. Inevitably, someone would invent them; the idea requires only a simple biological analogy. But once it would escape into the general culture, there would be no way back, and I didn't want to make my professional life around it, lucrative as it might be. The manufacturers of spray-paint cans likely feel the same way...

Consider that our cities will get smart and be able to track us with cameras on the street and with microwaves that read the chips in our phones, computers, even embedded beneath our skin. The first commercial use will likely be to feed advertising to us, as in the 2002 Steven Spielberg film *Minority Report*. We'll inevitably live in an arms race against intrusive eyes, much as we guard against computer viruses today.

Stuxnet, the virus known to have invaded Iran's nuclear facilities, is apparently the first malicious code deliberately designed to disrupt targeted industrial processes, mutating on a schedule to avoid erasure, interrogating the computers it invades, and sending data back to its inventors. Stuxnet is able to reprogram Siemens-manufactured programmable logic controllers and hide the changes it introduces into them. Commands in Stuxnet code increase the frequency of rotors in centrifuges at Iran's Natanz uranium-enrichment plant so they fly apart. Yet much of Stuxnet's code is unremarkable, standard stuff, lacking advanced cloaking techniques.

Still, it's a wholly new thing—a smart virus with a grudge—evolving, self-aware, self-educating, craftily fulfilling its mission. Expect more to come. Countries hostile to the U.S. could likewise launch malware attacks against U.S. facilities, using Stuxnet-like code to attack the national power grid or other critical infrastructure.

Though seldom discussed, U.S. policy has traditionally been to lead in technology while selling last-generation tech to others. Thus we are able to defeat our own prior inventions, along with sometimes deliberately installed defects we might exploit later.

It's a wholly new thing—a smart virus with a grudge—evolving, self-aware, self-educating, craftily fulfilling its mission.

Stuxnet looks like a kluge with inventive parts. It does not hide its payload well or cover its tracks. It will not take much effort to greatly improve such methods (with, say, virtual machine-based obfuscation and novel techniques for anti-debugging), whatever the target. Once major players use them in nation-state rivalries, they will surely leak into commerce, where the stakes are immense for all of us. If Stuxtype, untraceable malware becomes a weapon of commerce, our increasingly global commercial competitiveness will take on a nastier edge.

Meanwhile, if living in space becomes routine, the related systems will demand levels of maintenance and control seldom required on Earth. Consider that the International Space Station spends most of its crew time just keeping the place running—and potentially can be corrupted with malware. So can many systems to come, as our environment becomes smarter and interacts with us invisibly, around the clock. Increasing interconnection of all systems will make smart sabotage a compelling temptation. So will malware that elicits data from our lives or corrupts systems we already have, in hopes we'll be compelled to replace them.

Now think beyond these early stages. What secondary effects could emerge? Seeds of mistrust and suspicion travel far. But that's the world we'll live in, with fresh problems we'll be able to attack but only if we've thought them through first. C

Gregory Benford (gbenford@uci.edu) is a professor of physics at the University of California, Irvine, and a novelist, including of *Timescape*, winner of the 1980 Nebula and British Science Fiction Awards.