Most of the terms used for computer viruses are metaphors; they have a largely medical origin, and are seductive if not literally sexy. The very real worries we have about AIDS, for example, no doubt colour the way we talk about computer viruses. At the extreme, abstractly viruses are clearly just algorithms, and like any other algorithm they are good for some things and not good for others. This article tries to take a dispassionate view of viruses, despite the fact that almost all of the ones we've seen so far are malicious. If the views expressed here are as a result contentious, then so be it.

Communication and flexibility are the ecological niche of viruses and worms. Is there a tradeoff: can some of the benefits be made available without succumbing to the threats? Might some of the benefits outweigh some of the dangers? Despite the obvious disadvantages of viruses now, this article argues that they have—to a limited extent—a constructive role for the future. Optimistically, I think viruses are going to bring about several changes in computing which will be beneficial. Most people acknowledge that electronic vandalism at least exposes security loopholes and in the long run this is beneficial (unless the company goes bust on the first security breach), but there are other possibilities.

1. Bugs versus viruses: a case for professionalism?

So far as a computer user is concerned, there is no difference between a bug and a virus: that is, between an accidental program fault, and a deliberate, self-propagating fault. (In fact, I have lost far more data as a result of straightforward bugs in expensive proprietary software than from viruses.) Nothing will protect anyone from bad software, even if bought from reputable manufacturers.

Most software manufacturers provide a very dismissive warranty on their products: the only purpose of the warranty seems to be to protect the manufacturer from any liability whatsoever. It's worth looking at a warranty if you have not already done so:

"The software is provided 'as is' without warranty of any kind, whether expressed or implied including without limitation any implied warranties of merchantability of fitness for a particular purpose all of which are expressly disclaimed. The authors, their distributors and dealers shall in no event be liable for any direct, incidental, or consequential damages, whether resulting from defects in the disks, or from any defect in the software itself or documentation thereof. The entire risk as to the results and per-
H. Thimbleby/Can Viruses Ever Be Useful?

The performance of the software and materials is assumed by you. If the software is defective, you and not the authors, their distributors or dealers, assume the entire cost of all necessary servicing, repair or correction. This warranty provides you with specific legal rights."

And to cap it, I suggest you read the fine print on your credit card conditions: if your credit card company has any problems with their computers it’s your fault. If you think that the necessarily careful legalism gives an unfortunately negative impression of the quality of programs, see the discussion in [1].

Clearly, if any one manufacturer acted more responsibly it would put itself at a competitive disadvantage. But now that programmers can become members of professional bodies (and Chartered Engineers), it is time that they took as professional an attitude to their work as professionals in traditional disciplines—for instance, by accepting some liability for the work that they do. To change the status quo, there needs to be some very considerable pressure.

Perhaps that pressure will come from viruses?

While we let manufacturers hide behind their warranties like the one above, we will have little legal redress against deliberately malicious programmers. Indeed, the AIDS disk came with a so-called warranty.

2. Software Upgrading and Subscription

As vandals produce new viruses, so new anti-virus programs have to be developed or extended to cope with the new strains. Since viruses travel around so fast, it is extremely important that users can get upgrades to their anti-virus software as fast as possible. Typically, users subscribe to an anti-viral product so that they can easily get updates whenever a new virus hits the scene. So, viruses put the pressure on to make software upgrading easier. As I argued in ref. 2, software subscription is a good idea more generally and indeed might have a dramatic effect in reducing piracy.

3. New Computer Architectures

Viruses are getting both more widespread and far more subtle. It is conceivable that soon most personal computers will become practically unusable, or their users will have to become recluses so that they don’t get infected. The basic problem is that we buy computers to do anything, but actually only thinking of doing things like using spreadsheets and word processors. But because computers can do anything, in particular, they can (and unfortunately they do) run viruses. If we bought computers that could only do a few specific things—like a pocket calculator can only be a pocket calculator—then the computers simply would not be able to run viruses.

The solution appears to lie in a new design of computers, in particular dedicated products. But new computers that protect against virus infection have to be completely incompatible with all current computers! If they could run the same programs, then again, they could just as easily run the same viruses. So, viruses herald new, incompatible computers.

There are two ways to make incompatible computers. Another generation of hardware (say, RISC chips that can’t run any PC software) might be designed (with better security built in)—but then all these systems would be compatible with themselves and we’d merely have the same virus problems sooner or later. The other approach might be to make each machine unique: incompatible with everything else. This might be done by, for example, generating the microcode by some encryption process. Then any program to be run on that machine would need a password, but more interestingly no program on that machine—including viruses—would be able to construct programs to run on other machines. Viral infections would be contained. Maybe a public key encryption scheme could be used so that accredited
software suppliers could distribute software more easily than personal computer users.

Despite the overhead of passwords, there would be several direct advantages to computer users, the most important of which is that if viruses are unable to corrupt programs, then anything anyone else will also find it harder. And that includes the people who wrote the programs in the first place. If it is harder, practically impossible, to modify programs once they have been sold, then manufacturers are going to have to take a lot more care over them. They won’t be able to “patch them up” later.

4. Advancing Genetics

Bacteria, like viruses, were first noticed because of their disruptive effects (like souring wine or causing diseases), only later did anyone realize that they are essential for life, with functions ranging from fixing nitrogen, to helping digestion. By analogy, it has recently been suggested that biological viruses may actually be useful. Maybe there are viruses that we have still to discover that have an essential part in life?

A long-standing problem in evolutionary circles has been how speciation occurs. A species is a group of animals that cannot reproduce with another species. So how does mutation successfully bring about a new species when you need the rather unlikely occurrence of two mutants capable of reproducing? Furthermore, how do birds, say, evolve from reptiles, a change requiring several mutations (feathers, lighter bones, and so on), none of which are, on their own, beneficial for reptiles?

A neat answer to both conundra might be to invoke viruses. Speciation (the creation of new species) might arise by infection: the infection affects a large number of individuals (so they can interbreed), and this could easily mutate several features of the individuals at once. These are interesting, perhaps contentious, issues for geneticists. But might computer viruses have advantages that, so far, have gone unnoticed because of the antipathy surrounding them?

It has been argued [3] that, in the biological case, invading creatures (such as viruses and the precursors of mitochondria) became assimilated into their hosts, eventually performing vital functions. Will viruses—in some form or other—eventually become assimilated, perhaps as the basic communication and information processing units?

Perhaps work in genetics will influence work with computer viruses. Or maybe the reverse: in principle, computers are a lot simpler than biological organisms and theoretical insights about virus behaviour (about evolution, maybe about the processes of life in general) may be easier to come by in computing contexts. So the computer security threat of viruses might lead to advances—who knows?—in human immunology. That would be a very real benefit and probably worth all the fuss we have with computer viruses.

Most computer viruses are perverse; some, indeed, have been claimed to be “accidental”—rather as accidental releases of pathogens from biological research laboratories might be. One advantage of our awareness of the danger of computer viruses might be to reduce the enthusiasm for genetically engineered biological products. The probability, based on our experience with computer viruses, that they work out as rapidly replicating, uncontrollable pests seems considerable.

5. Advancing Sociology

Biology is one science that stands to benefit from the high profile of “biological” problems in computer systems. Sociology is another discipline that should get increased attention.

Hacking is a complex social phenomenon. I am not a sociologist, but it seems that some of the problems of viruses might be better investigated by sociological or psychological research—aiming to address issues surrounding the creation of viruses rather than the “after the horse has bolted” approach of improved computer security. So I hope that viruses result in more
Can Viruses Ever Be Useful?

funding in this neglected area! Sociological insight into deliberately malicious behaviour would probably also give insights into “accidental” bugs; certainly if better programming environments could be designed that were is some ergonomic way more conducive to writing correct programs, perhaps this would also influence hackers for the good?

6. Autonomous Communications

Computer viruses are virulent because they don’t tell you what they are doing—of course, if you knew, you’d stop them! Their virulence is perhaps one of their most alarming features: in practice it means that any close group of computer users may simultaneously cease being able to work at all on their computers. We don’t need to exaggerate the dangers to paint a very gloomy picture indeed.

Computer viruses have two features that make them effective: they are autonomous and they communicate. By autonomy, I mean that viruses get on with their work without interference or guidance from the computer’s user—of course, if viruses were not autonomous, users would never give them permission to replicate and spread! By communication, I mean that viruses rapidly spread their particular disease, typically by infecting floppy disks (worms use networks).

There are all sorts of occasions when the computer user would like to have autonomous communication but instead working on his own behalf. Ian Witten, of Calgary University (Canada) and I have been working on this idea, which we have called Liveware. Liveware, then, is practically a benign virus mechanism…but it is potentially so useful that it is best to forget the analogy with viruses! Liveware works like a virus in that it also replicates and spreads but it carries information on behalf of the user, or on behalf of a group of users wanting to share their work. There are too many advantages to this scheme to cover properly here, but see ref. 4. Briefly, liveware is exactly what all these new gadgets, programmable telephones, smart cards and so on are going to need in a world of mobile users.

References