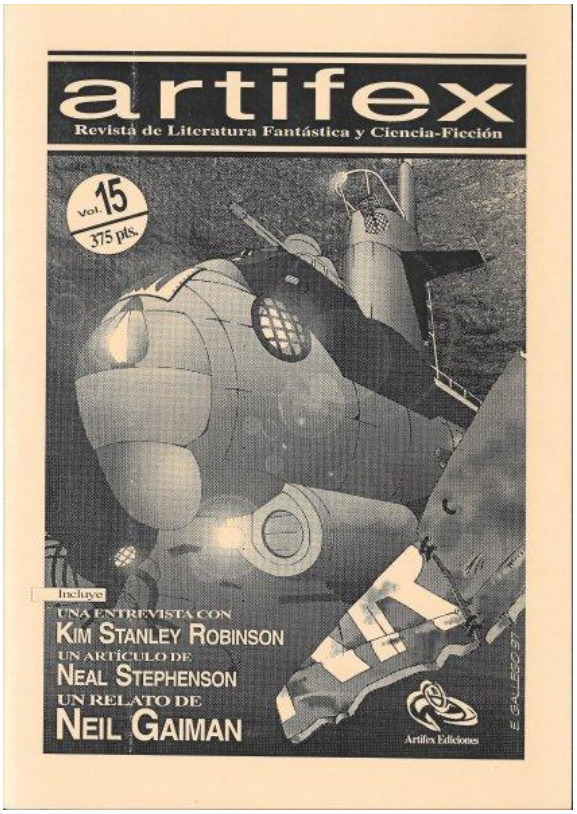
Dreams & Nightmares of the Digital Age

Neal Stephenson



1997

In The Diamond Age, science-fiction novelist Neal Stephenson imagined a world in which hyperadvanced microtechnology is wedded to the social structure and mores of the Victorian Era. Currently at work on a new novel about electronic secrets, Stephenson took time off to prepare for TIME this admittedly speculative rumination on worst-case scenarios for the networked society.

Worrying about technology has become one of the pillars of the Establishment. Our government has created special panels and subcommittees for it. It tends to come up with ideas like the Clipper chip (a way of controlling cryptographic technology) and the V chip (to control children's access to nasty television programs). When the government becomes paralyzed by bickering and partisan maneuvers (which is how we Americans like it), it's always safe to roll out a new chip; in today's techno-mythology, chips are like tribal fetishes that can be waved around in times of stress as a vague indication that something is being done about some troublesome informational problem or other.

Recently a lot of worrying has been done about the Internet. People who are concerned about anarchy tend to see it as a thrumming hive of villainy, where crazed extremists exchange nerve-gas recipes and whip themselves into a frenzy by exchanging faulty information about black helicopters. People who are fearful about government see the Internet as the perfect tool for Big Brother.

If the Internet had gone wrong in just the right way, either of these might have resulted. But it hasn't. My own recent efforts to find a nerve-gas recipe on the Internet were fruitless. When you want information on the Internet, either you know exactly where it is or you don't. If you already know where it is, then the fact that it happens to be on the Internet is irrelevant; you could just as well get it by fax or mail. If you don't know where it is, you have to use a piece of commercial software called a search engine. You type in a few key words or phrases, and the engine tries to find World Wide Web documents that contain them. When I tried this, the search engines turned up either sheer noise (documents in which the words nerve, gas and recipe happened to appear separately) or references to the concept of nerve-gas recipes.

The Internet is the only place where worrying about something makes it less likely to happen. Every time someone posts a message to a newsgroup about the danger of nerve-gas recipes on the Internet or a journalist writes an article (like this one) about the same topic, which is then available on the Internet, a little more noise is added to the system, and any would-be terrorist who tries to search for a nerve-gas recipe finds literally hundreds of thousands of red herrings.

Even if a person were able to download a string of words billed as a nerve-gas recipe, he'd face a real dark night of the soul if he got the ingredients together and sat down to mix them. Considering how hard it is to trust, say, the butcher in the era of E. coli outbreaks, who is crazy enough to trust an anonymous recipe that, if it goes wrong, will kill him? The very anonymity that makes it possible to post nerve-gas recipes makes the people who have posted them untraceable and unaccountable and hence difficult to trust. Ted Kaczynski has not yet been proved to be the Unabomber, but if

he is, we may one day see him as the very model of an Internet-age terrorist, circa the early 1990s, in that he totally ignored the Internet.

Crypto (cryptographic technology on the Net) is going to change that, however. If we're going to worry about a technology, let's worry about crypto.

Crypto is a collection of protocols. "Protocol" here means a set of rules governing an exchange of data, agreed to by all participants. The number of core protocols in crypto is fairly small. One example is the digital signature. Data can be given a digital signature that, like an ink signature on a contract, verifies that they were signed by a particular person. It is stronger than an ink signature because it proves absolutely that the data have not been meddled with. Another protocol is public-key encryption, which, to make a long story short, can encode documents so securely that no government on earth can decode them in a reasonable amount of time. These and a few other basic protocols can be combined to make more complicated ones, such as digital cash–a system for transferring real money (not just credit-card numbers) from one person to another, anonymously and untraceably.

An advanced protocol that has been getting a lot of attention from high-technology developers has to do with reputations. Anyone who has found his E-mail box filled with junk mail or done a Web search that turned up hundreds of thousands of irrelevant documents may have wished that his computer would select only the stuff he finds interesting. This reduces to a problem of assigning an unforgettable reputation–an index of reliability, tailored to the user's personal interests and biases–to the source of each piece of information. This in turn hinges upon digital signatures.

Put it all together, and in a few years we might have something to worry about. Someone searching for a nerve-gas recipe might be able to tell his search engine, "Show me only the good stuff," where "good" means that which is highly regarded by fellow terrorists. The recipe would arrive encrypted so securely that no government-watchdog agency could read it. The digital signature would prove that it came from a well-reputed chemist and that its contents had not been tampered with en route. The terrorist could mix up a batch of the stuff, leave some sealed in a container in a public place and then send untraceable E-mail to the authorities telling them where to find it and demanding that a certain ransom be paid lest more be dumped into a subway vent during rush hour. The payment would then be made, not through an exchange of cash but through an untraceable, digital-cash transfer to an anonymous electronic bank account–with no risk to the terrorist.

There is almost no limit to the ways in which generalized cryptographic technology could be used by bad guys. Wiretapping will be removed from law enforcement's tool kit as crypto telephones–the ultimate scrambler phones–become widespread. The battle to control electronic transmission of child pornography will soon be lost. It will be much more difficult to track down drug dealers by following their money trail.

All this presumably explains why the U.S. government has long been worried about crypto and has tried to combat its spread with increasingly foolish measures, such as declaring cryptographic software to be a munition. From a careers perspective, a

crypto programmer with a non-U.S. passport is a good thing to be. Nearly all Silicon Valley companies must build some form of crypto into their products to make them competitive. Since U.S. regulations forbid the export of such technology, these companies simply farm out that portion of the work overseas. To the extent that the U.S. ever had any proficiency in crypto, we are now exporting it without getting anything in return.

Naturally we look to our government (for all its faults) to exercise some control in these situations. But one thing that makes crypto unique is its potential to cripple government as we know it. Governments can't function without revenue, which they get mostly from taxes. Hence large tax-collecting agencies exist that have exceptional and, to many people, creepy snooping powers. The spread of electronic cash will eventually give everyone the ability to carry out most of their financial transactions behind a cloak of anonymity that no government agency can pierce.

Any effort governments can make to combat this problem will require money, of which they will be collecting less and less. Once the government gets on the wrong side of this feedback loop, there's no way out of it, short of instituting some kind of pervasive totalitarian system.

Few tears would be shed for the government in Silicon Valley, where libertarianism is popular. But in the long run anarchy on the local scale (militias) or the global scale (organized terrorism by outlaw states) is a more serious threat than Big Brother. And it's hard to see what the libertarian approach has to offer on this front. One of the best ways to discourage terrorism is by threatening massive retaliation against sponsor states, but this doesn't work without a powerful central government running a big, sophisticated military. Crypto-savvy citizens who will find ways to avoid paying taxes in the future may feel that this is reason enough to make voluntary contributions of not just money but also time in uniform.

The threat of retaliation is only so effective, though; beyond that the only way to prevent terrorist acts is through surveillance of everyone and everything. This might seem incompatible with the general antigovernment trend. But terrorism is deeply disturbing; anything that appears to combat it is reassuring; and the citizens of a libertarian Utopia may one day eagerly accept such surveillance. Having failed to sneak in through the back door, Big Brother may return via the front and be welcomed.

Crypto may offer at least one solution to this ultimate nightmare. There is a cryptographic protocol called secret sharing, which is a way of dividing a piece of information (let's say a stream of bits representing digitized video) into several pieces, which are called shadows. The shadows can be distributed among several recipients. A single shadow or several combined are unreadable gibberish. In order to reconstruct the original information, the shadows of all the recipients must be put together.

Now imagine a digital-video camera on every block, directing its output into a tamper-proof chip that divides it into several shadows. One shadow goes to, say, the local police department, one to the local block-watch group, another to the American Civil Liberties Union. As long as any one of these groups withholds its shadow, the

information cannot be reconstructed; it effectively does not exist. It's as if there were no camera. But if a crime takes place in view of the camera–let's say the terrorist puts down his nerve-gas sample in front of it–then the groups can combine their shadows to re-create the original video and catch the terrorist in the act. Implemented on a wide scale, this could make it very difficult for a criminal to get away with a crime. And as long as at least one shadow holder is responsible, the privacy of citizens would not be threatened one whit.

As new technologies continue to appear, we will probably see a lot of initial enthusiasm, followed by a rush of anxiety as we realize how evil people could use them, and then a gradual relaxation as we come to understand how the technologies could also be used to thwart the bad guys' schemes. This works, of course, only as long as the new technologies are mastered by curious people–such as the millions of personal-computer owners who in just a few years have transformed the Internet from a small government-research network into a new global-communications medium. Bad guys are notoriously fascinated with toys, and nothing will frustrate them more than finding that after they've surged forward into new realms of technology, those territories have already been charted and colonized by stubborn hobbyists.

Why don't the bad guys ever seem to get there first? Sometimes they have come worrisomely close, as in the weapons laboratories of the Third Reich. But in the end technology is based on science, and science is a uroboros, the legendary worm that, according to the lore of alchemy, encircled the earth, forever eating its own tail. It is an eternal process of consuming and destroying its own dogmas. This can work only where the free and open expression of ideas is fostered. It is no coincidence that science has flourished in the freest countries and that totalitarian societies eventually lost their scientific edge as new ideas were put through an ideological filter and good minds were diverted into politically motivated nonsense such as Lysenkoism and Aryan eugenics. It is tempting to see manifest destiny in this, to conclude that the mutual reinforcement of free societies and technological prowess is more than just dumb luck. That is the vision of the future that is implicit in Star Trek.

Cyberpunk novels take a decidedly different view of the matter. In case we are just on a lucky streak, those of us who believe in the maximum amount of freedom for the maximum number of people had best make the most of it, lest the next century's dictators catch us napping.

Neal Stephenson
Dreams & Nightmares of the Digital Age
1997

Translation of ‘Sueños y pesadillas en la era digital’. In the volume ‘Artifex 15’, Luis G. Prado Editions, Artifex collection, Number 15 (1997). Translator: Luis G. Prado.