The name of Markus Hess was given. Last month a West German by the name of Markus Hess was given an 18-month suspended sentence after being found guilty of a bizarre series of international computer hacking offences. Ironically, he and his associates in the Kaos Komputer Klub had been selling information on American military-base computers to members of Eastern European security organisations who have, by now, radically altered their strategic outlook, been thrown in jail, or been elected to parliament - take your pick.

While the Cold War which generated this particular incidence of hacking might have changed, the issue of who gets access to the vast and powerful computer networks which run around the globe is here to stay. Perhaps a new geography of information politics might take the place in part, at least, of the old Cold War territories.

Clifford Stoll, the man who tracked down Markus Hess, has pioneered experimental study of hacking as a phenomenon and is one of the first to attempt to articulate these issues for a wider audience in his book The Cuckoo's Nest. It reads like a high power global detective story - which, in fact, it is.

Tuesday, June 23, 1988: West German police seize computer equipment, discs and printouts from an apartment and a company office in Hanover. Shortly afterwards, Markus Hess is picked up by police for breaking into American military computer networks to collect passwords and other information. Kaos was allegedly selling the information to KGB agents in exchange for large amounts of cash and cocaine. Hess was using an elaborate series of computer networks, exploiting a few simple bugs in system programs. He was even able to consume a large amount of free computer and network time using the accounts of a large American defence contractor. Ironically, Hess was detected when Stoll found a 75c error in a billing system for computer time.

Bill Landreth is also a hacker, but of a slightly different kind. In his book The Cracker he presents an image of the cracker-style hacker as the loner, the outsider, prowling the frontiers of the computer networks. Like a figure from a Hollywood western, the hacker knows a technologically dynamic landscape with few laws or customs. A new world without a history, where everything has to be invented on the moment, if not exactly on the spot. (There is no spot exactly. The hacker moves in a logical space which is only incidentally a movement in geographical space. They move in an information landscape, sometimes called cyberspace.) The hacker is a tester of limits, an unwanted guest in the system. The system is a host to be pushed to the limit but not destroyed. Landreth is very clear on the ethics of this kind of hacking: never destroy other people's data. The hacker appears within the system to look and learn, and to prompt the host organism, the computer system and its system managers to react.

Not all hackers are quite so ethical, however. Some leave behind 'logic bombs'. Clifford Stoll recounts an instructive story in this regard in his book The Cuckoo's Nest. It starts with a phone call at 2.25 am from Gene Miya at NASA Ames Laboratory: "Help! Our computers are under attack!". Stoll put the phone down and it rang again. This time, when he picked it up, it just beeped. Morse code from his own computer at the Smithsonian Institute for Astrophysics, Cambridge, Massachusetts. His computer was under attack too!

Stoll represents another version of the hacker figure. The hacker as a legimate user and manager of computer systems who solves problems, who keeps the system not only running but innovating. Stoll had a reputation for coming up with ways to foil the other kinds of hacker, the Landreth and Hess-style crackers. So he was a logical person for Gene Miya to call. Stoll made some calls and discovered other networked computers were being attacked by a virus. He tried to log onto a computer at the Lawrence Berkeley Laboratory, California, where he used to work as a system manager and where his anti-hacker hacking career began. Stoll typed in a command he picked up from watching his Kaos hacker foes at Berkeley, and found that the Berkeley computer was infected. This gave him his first clue to the nature of the virus: the computer was interfacing wildly in all directions, trying to talk to every other computer it could reach. With the computer trying to connect to every other computer, the flow of information was becoming a cacophony of noise, making the flow of information impossible, slowing the computer's processing down to a crawl.

Every time Stoll tried to shut down the connections, new ones would spring up. Like a biological virus, this one entered a system, replicated itself, and sent off copies to other computers. Many computers are linked together through networks such as Arpanet, which connects eighty thousand computers.

Computers have security systems to prevent noise of this sort getting in and ruining the system, but this virus infected some six thousand before being brought under control. The virus had been designed to exploit a security loophole in the electronic mailing system. Over the next couple of days, 'white hat' hackers battled this lone-gun 'black hat' across the United States. Some began unwinding the machine code discovering how it worked and what exactly it did. Others wrote 'patches' to cover up the loopholes in the operating systems the virus exploited. All this information was exchanged across the country on electronic bulletin
boards. In the space of a couple of days, all that was left to be discovered was who wrote it. It turned out to be a student at Cornell University, Robert Morris jr, the son of the Chief Scientist at the National Computer Security Centre, the only public part of the shadowy National Security Agency. The mob who are supposed to set the standards of computer security. What a Freudian nightmare!

Scientific computer systems tend to be very open networks, without elaborate security precautions. This allowed Hess and Landreth and the virus to slip through a loophole in the net and get into scientific, medical and even military computers, although not highly classified ones. Networks rely on trust, or mutual consent between users about the correct use of the system. While they are relatively democratic systems for those with access to them, many people are excluded. Hence hacking raises complex ethical and political problems, many of which were recently discussed on an electronic bulletin board for Harper's Magazine (March).

The fact that Hess had been through literally hundreds of computers on the extensive American scientific and military networks - and not just American computers in America, but also base computers in Japan and Alaska - meant that security would subsequently be tightened on scientific computer networks and information would flow more slowly. Hence, one can say that there is a broader, more abstract kind of logic bomb at work here: no matter how open a network is, no matter how democratic, somebody is being excluded.

As philosopher Michel Serres insists, one only produces the passage of information between two people by excluding a third: by excluding the noise of other parties who want to be heard. Noise will struggle to enter the system, and for any number of motives. The Russians want information. The hackers might want money or glory or a good supply of coke, or some kind of oedipal rupture, who knows? In any event the ever-present threat of noise is the logic bomb within the system. The ethical question is whether noise is always necessarily a bad thing, or whether it has creative uses.

The idea of a logic bomb is useful as a suggestive metaphor for how complex information networks function - and dysfunction. There appear to be logic bombs in all kinds of information networks that were not consciously programmed. They are activated when noise traverses the old boundaries and territories that used to characterise social life. These logic bombs are programmed into the information networks as an accidental byproduct. They are a byproduct of the complexities of power in an information intensive world. They are an unconscious form of negation. They are the unintended effects of planned rationality and the inevitable byproducts of conflict within the institutions which govern cyberspace. In a world where the networks are run by bureaucracies, and worse, where information about our credit ratings, sexual preferences, political affiliations, work absentee records and health are not even handled by bureaucracies but processed by machine, hacking becomes both a threat to individual privacy and a tactic for breaking through the secrecy of government data and the patent and copyright restrictions of the big corporations.

A little disorder in the networks might be essential to preserving liberty, and also for advancing the tools and technologies of information systems. As St Just put it: the disorder of today is the order of tomorrow. Or as one of the hackers in Harper's said: "There's a hacker born every minute".

McKenzie Wark.

JUDY HORACEK

The idea of evolution as progress towards increasing perfection has long been discounted by enlightened thinkers. Now read on...

LESSON ONE

The Evolution of the Cotton Bud

INVERTEBRATE Stage 2
Amoebic State
'The Cotton Ball'

INVERTEBRATE Stage 2
Exo-Skeleton
'The Tampon'

VERTEBRATE
Internal Spine
'The Cotton Bud'

So, although tampons are lower on the evolutionary scale than cotton buds, they cost fifty times more, in the same way as crayfish costs more than flake.