Department of Defence—use the security community's so-called "Orange Book" software to protect themselves from serious mischief. When the defence department's cyber-security team attacked 3,000 of the Pentagon's own computers, only 5% of the people operating the target systems detected the intrusion.

The Rand researchers see cyberspace as rather like the Wild West. With little law and order, the first thing to do to protect a network from cyber-attack is to rely on trusted friends—ie, enclaves of computer systems that comply with rigorous security measures. The conventional view is that, around these fortified enclaves, network managers need to build a stockade (or firewall, as it is known in the trade). Only the most trusted communications from the outside world should then be allowed through the firewall. Even e-mail messages need to be screened carefully. Lately, logic bombs—programs designed to cause havoc when a specific set of conditions is met, such as the computer executing a particular sequence of instructions, or it being a particular time and date—have started turning up as attachments to apparently innocent electronic messages.

But a whole new school of thought on cyber-security is emerging. This seeks to mimic a biological immune system. Like a living organism, a public network is made up of lots of complex, diverse and highly interdependent components. Like such an organism, it cannot predict what kind of attack it might suffer next, nor how the infection might evolve. Because the organism cannot simply disconnect itself from the world, it protects itself with a combination of semi-permeable firewalls (a skin and cell membranes), sensors (antigens) and circulating killer agents (antibodies and white blood corpuscles).

The implication for cyber warfare is that erecting perfect barriers around public networks is not only impractical but probably undesirable. Mr Hundley and Mr Anderson reckon that imperfect barriers backed up by active defences may provide better protection. They are intrigued by the possibility of developing software agents that function like antibodies.

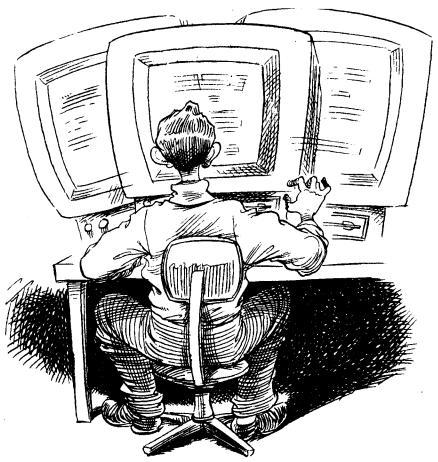
The defence department will not say whether it is developing active measures for going on the cyber-offensive. The work is a "black" programme hidden from congressional oversight. But the theoretical danger of cyber war has put the country in an odd position. Military planners normally want to be ahead in the technological game but, in a way, the more "wired" a country is, the more vulnerable it is to this sort of attack. Maybe America's best defence is to encourage potential enemies to become equally dependent on information technology. Then there would be scope for retaliation. ■

Quantum computing

Two-bit heroes

COMPUTERS may be fast, but they are stubbornly single-minded. Their central processing units can cope with only one instruction at a time. Usually this does not matter. Stupidity is more than made up for by speed. But for the biggest calculations—those involved in modelling the earth's climate, for example, or in breaking modern ciphers—it is necessary to wire up many processors in parallel in order to arrive at a result this side of doomsday.

That is far from satisfactory. Such arrays are difficult to design and in general they have to be connected in a particular way for each application. On the other hand, a processor that could run on traditional lines and yet cope with more than one thing at a time is difficult to conceive of. So it is appropriate that many of those who are trying to do the conceiving are also trying to understand another difficult concept: the quantum-mechanical idea that something can be several different things at once.



This is a slight simplification. What quantum mechanics (which describes the behaviour of atoms and their component particles) actually says is that until they are measured or disturbed in some way, a particle's properties—such as its energy, angular momentum and even position—do not possess definite values. Instead, they exist as a "superposition" of possible values.

Quantum computing aims to take advantage of this capacity for simultaneous existence in multiple states by allowing a single switch to be both on and off at the same time. Since computer processors are just large networks of switches, this would be a snazzy trick. Many different processes could, in theory, be carried out simultaneously on a single network.

In the past year researchers at the National Institute of Science and Technology (NIST) in Boulder, Colorado, and at the California Institute of Technology in Pasadena have taken the first halting steps towards this ideal. Both teams have built systems in which one characteristic of a single quantum object—such as an atom or particle—is used to change another of its characteristics. This type of interdependence is known as conditional dynamics and is the basis of the logic gates that lie at the heart of computers. Both the Caltech and the NIST experiments involve dynamics which could be used to make a controlled "not" gate.

"Not" is one of the mathematical operators used in the logical system known as Boolean algebra (others include "and" and "or"). Many mathematical problems can be expressed as long strings of Boolean algebra. Computers solve problems using networks of switches to perform Boolean operations. A controlled "not" gate is a switch with two inputs: a control bit and a target bit. When the control bit is on, the gate performs a "not" operation on the target bit, switching it over from on to off or vice versa; when the control bit is off, the target bit is unchanged.

The NIST group, led by Chris Monroe, has used a beryllium atom as its quantum object. The atom is cold (a few thousandths of a degree above absolute zero) because quantum effects are difficult to detect above the background noise at higher temperatures. But with the atom trapped electromagnetically at this temperature it can move only slightly, in one of a few vibrational modes.

The control bit is stored in two of these quantum-motion states. The atom can be moved from one state to the other (corresponding to "on" and "off") by firing a laser pulse at it with energy equal to the gap between them. The target bit is the internal energy state of the atom, which depends on the direction of the spins of its electrons. The two values of the target bit correspond to the electronic ground state, which is the state with the lowest energy, and the first excited state, when one electron flips its spin. This flip represents a switch in the value of the target bit, and it happens when the control bit is given the value "on" by setting the atom in its first excited motion state.

At Caltech, Jeff Kimble and Quentin Turchette use polarised photons as their quantum information carriers. Two beams of photons are made to interact by shining them through a stream of caesium atoms. One, the control beam, affects the optical properties of the caesium atoms in such a way that the angle of polarisation of the photons in the second, target, beam may be flipped, or not, depending on the first beam's signal. The same sort of conditional logic may then be deduced as from Dr Monroe's beryllium atoms.

So far, so ordinary: these could be no more than clever ways of making a normal, unambiguous Boolean logic gate. Except that, because the "on" and "off" switch po-

sitions are in fact quantum states, a gate built around the NIST or the Caltech experiments could be in a superposition of its possible settings. If its input were such a superposition, its output would be too. Until a measurement made it "choose" one condition or the other, such a gate could hold information on the results both of operating as a "not" gate and of not doing so. And were it part of a larger circuit, it would be able to pass on this superposition to subsequent gates, allowing the circuit to process several versions of a calculation at once.

The next steps will be to demonstrate superposition in a working gate and then link several gates together. This will be tough. Joints expose a system to the risk of external noise. Wires can carry heat into a system. Laser beams may introduce wobbles as their power fluctuates minutely. Such noise would wipe out quantum superposition, dashing any hope of maintaining several logical states at once. And even if they succeed, the quantum mechanics face another hurdle. How will they get a result out of a quantum computer without destroying its quantumness by measuring something?

Early in 1994 Peter Shor, of AT&T Bell Laboratories in Murray Hill, New Jersey, showed a way that this could be done for some kinds of problems. He devised a mathematical procedure for factorisation using quantum logic.

Factorisation (finding the prime numbers that multiply together to make another number when you only have that other number to start with) may not sound like a leading-edge mathematical problem. But modern ciphers are based on the products of pairs of large prime numbers, and cracking them is big business. To break such a cipher a spy must first factorise this numerical key. That takes time, even for fast computers. In 1994 a battalion of 1,600 linked computers around the world needed eight months to produce the prime factors of a 129-digit number. Matters deteriorate as the problem scales up: the same apparatus would take about 800,000 years to factorise a 250-digit number.

Dr Shor demonstrated a way to arrange these calculations so that if they were done simultaneously, as a superposition of evolving quantum states, likely prime factors would tend to stand out and crop up often when measurements were taken. Running the calculation several times over (which would be feasible because it would take so much less time than on a conventional computer), and applying statistical analysis to the results of the measurements, would produce the prime factors.

Even so, running Dr Shor's procedure on a 200-digit number would require thousands of quantum bits joined together. For now, the would-be quantum hackers are happy to have linked the first two. ■

Electric cars

Low-impact vehicle

DETROIT

AFTER years of false starts, General Motors has at last set a date for putting its first battery-powered car into production. The EV1 that will roll out of GM's factory in Lansing, Michigan, later this year will be the first car in modern times to have been specifically designed by a big car maker to run on electricity.

The timing is intriguing. GM has announced its decision just as California's regulators are preparing to relax the strict air-quality standards that were an important reason for going ahead with the project in the first place. The California Air Resources Board decided in 1990 that 2% of the vehicles sold in that state by the seven companies with the largest market share would have to be emission-free—in other words electric—starting in 1998. By 2003, the board wanted the figure to be 10%. Now it admits that "new studies" have shown what everyone else knew all along: that its mandate would be impossible to meet using existing battery technology.

This is because, without official bullying, people are reluctant to buy electric cars. Although the EV1 has been loaded with all sorts of baubles—dual air bags, air conditioning, power windows, even a CD stereo system—it is far from clear that these will compensate for a puny range, the basic flaw of every electrical vehicle. Publicly, GM officials claim that the car will have to be recharged every 145 km (90 miles) or so, but they concede privately that the real figure is likely to be nearer 100 km. Without access to a high-speed charger, such a refill will take around 15 hours.

Even squeezing this much range out of the EV1 has required a lot of engineering sleight of hand. Around 400 kg (900 lb) of lead-acid batteries are secreted about its body. To help compensate for all this weight, and to maximise the distance it can cover, the vehicle is equipped with low-rolling-resistance tyres, an aluminium chassis, a wind-cheating plastic skin and a regenerative braking system that helps to recapture energy normally lost when the brakes are applied. Even the tear-drop body shape should cut down wind resistance. It is, in other words, a production version of the five-year-old "Impact" concept car.

Owners of an EV1 will have two ways of charging it. Those without access to a 220-volt power supply (most American domestic circuits are 110 volts) will have to do it the hard, 15-hour, way by plugging into a normal socket in the boot. But the preferred method is more ingenious: use of a paddle-like contraption that is inserted into a small slot in the car's nose. This operates by induction, eliminating the risk of sparks that might ignite the hydrogen released during recharging.

At 220 volts the paddle can give an EV1 the electrical equivalent of a full tank in three hours. Super-charged versions of the device, designed for use in service stations, shopping-malls and fast-food restaurants, can bring the batteries up to 80% strength in a mere 15 minutes. The fate of the EV1 could

An old-fashioned version