The devil in the machine

By Duncan Campbell

The Age, Sunday 9 January 2000

Never will there be general agreement on whether we escaped massive disruption through magnificent preparedness or whether the new century's high priests successfully pulled off a multi-billion dollar scam. But one conclusion is sure - the worries we have lived through belong less to technology and more to primal ideas in collective consciousness.

Now that the "bug" has bitten the dust after an almost eventless week, most people believe that billions have been swallowed up by hype.

The bug was not a fraud. But it was grossly oversold. Governments allowed, often encouraged the appraisal of its effects to blend smoothly into ever-amplifying prophecies of global disaster, whose cultural antecedents run deep in religion and history. Nor were the technological doomsayers blind to self-interest. Although few allegations of explicit fraud have emerged, there is no denying the abundant earnings Y2K computer specialists have enjoyed over the past two years.

The gradual change in their terminology should have warned us where we were headed. In 1997, it was the "year 2000 date problem". Then, "Y2K". Finally, it became the "millennium bug", easily endowed with trappings of Nostradamus and millenarian fantasy although lacking entirely the critical capacity of any pestilence to replicate and multiply - except, of course, as an idea of the human mind.

Doomsayers and government emergency planners fed off each other. In May 1998, the "Y2K Weather Report" from a Washington area computer company warned, "As 1999 progresses, as the global economy continues to decline and as more and more of the early Y2K failures occur, there will be some sudden, critical failure [that] will trigger a social crisis ... Whatever the cause, governments all over the world will seize on this as an excuse to put their plans for martial law into effect."

A year later, American journalist Jack Anderson alleged that the United States Marines were doing exactly that - secretly rehearsing to suppress civil unrest. In the same month, the US Department of Defence issued instructions requiring "prudent action to ensure its ability to meet its national security responsibilities and to respond to requests for assistance from civil authorities The Y2K problem has the potential to involve a large number of events that occur over broad geographic areas within a short time frame". Washington DC area civil authorities issued advice to its citizens to prepare for weeks without essential services.

THE TRUTH is that we have been living with the bug for years, and in some industries for decades. Had it been going to bite with a vengeance, we would have seen and been affected by the results long before sunrise on 1 January 2000.

The Y2K problem has customarily been presented as being derived, automatically and inevitably, from computer hardware or software operating with two-digit instead of four-digit numbers representing the year. Of itself, that isn't any problem, any more than if you date today's letters 5/1/00, when last week you wrote 28/12/99. Whether the letter is written by pen or processor, there is no problem in sending or understanding.

Significant problems arise only when calculations are made to compare two dates and a false result is then obtained. Then, will anything fail? Will it matter? Can it be put right? The most important questions of all have seldom been publicly tackled. What range of dates in a particular type of system can create an error? What is the natural period of the system that can create errors? How soon, before or after 1 January 2000, can problems arise?

Actuarial programs used by insurance companies have been looking past the year-end of 1999 for decades. If a non-compliant 1975 program had calculated how much in premiums a 20-year-old should pay up to retirement in 2020, 45 years hence, and come up with a negative answer, the problem would have been obvious - and fixed - before many of today's Y2K experts were out of nappies.

Y2K events have been noted since the mid-1990s. One early incident was in March 1997, when some US Department of Defence computers sent notices to contractors

ordering equipment for delivery in January 2000. The systems monitoring whether deliveries came in on schedule, noted the 21st century dates, miscalculated that deliveries were 97 years overdue, and issued the contractors with delinquency notices for their failure to deliver equipment just ordered.

This incident was one trigger for the Y2K scare. But if the scale of our recent fears had been justified, each passing month closer to January 2000 should have seen more and systems fail in this way, as date and time loops in forward-looking programs of every type crossed the millennial boundary. If the social consequences of some of the problems were to be as bad as predicted, some grave events should have occurred well before late 1999. None did, even before the billion-dollar bug industry got under way.

Events that did occur were not grave or irremediable. Another date that had been predicted to bring about widespread program failures - 9 September 1999 - passed without incident. This date was known to have been used in early programs as a "stop" point.

On 1 October 1999, four US Government departments did encounter problems. Computers dealing with budget information at the Energy Department, the National Science Foundation, Justice Department and Federal Aviation Administration either failed or sent out erroneous information. The reason was that 1 October marked the start of the US federal fiscal year.

The most worrying systems are those that have very short time comparisons, meaning that their effects would only have been observable close to midnight. If important control systems - power engineering, essential medical equipment - operating on tight time loops were using invalid dates, and were not checked and corrected, failures would have been serious. Here, detecting and fixing Y2K problems did matter, and could not be left to chance.

This history is why, months ago and for many systems, the little yellow bug should have been squashed and forgotten. It is also why doomsayers are still saying that Y2K isn't over, and that the road to 2001 is strewn with glitches. Date calculation errors arise only in systems that look forward or look back, and where some real

world consequence depends on the result. They are still overstating the case, since any system that looks backwards is already operating within the new century. There will be even fewer failures in the year ahead than in the year just past.

AS NEW YEAR approached, Y2K early warning screens stayed blank. But new horsemen were found. The FBI and the US "National Infrastructure Protection Centre" advised businesses that "cyber-terrorists" and anarchists would try to mark the end of the millennium by sabotaging computer systems. Some of Britain's biggest companies turned off their e-mail because of US reports of a wave of computer viruses and a massed hacker attack.

Since 1 January, no new `Y2K viruses' or mass attacks have been reported. Like everyone else, the hackers have been busy partying.

The scale of Y2K problems were comprehensible, calculable and testable. The millenium bug was the devil in the machine, to be seen first in the East. This was a saga from the centuries-old, Christian calendar-based myths of comets, second comings and satanic uprisings, not from the Silicon Age.

Duncan Campbell, based in Britain, is a journalist who specialises in technology issues.