

Computing that doesn't compute

Hire in some hi-tech firm, sack government staff - and queue for your passport for days

Duncan Campbell
Tuesday June 22, 1999

The passport agency is in the limelight for computer bungles as hundreds of holidaymakers are forced to queue for days in the hope their passports may be produced in time to travel. It's just two years since the agency struck a £240m deal with Siemens Business Services to automate passport production. The British system was to be franchised around the world. There would be digital data strips, automatic processing, even (allegedly) unforgeable holographic images. So confident were the agency of succeeding that scores of staff were laid off.

Under the exacting standards of Labour's private finance initiatives, this counts as an achievement and an improvement in "efficiency". More bungling has been detected in the heart of the secret state, with a Commons committee delivering a final obituary on the now dead and buried TRAWLERMAN computer.

This top-secret system was to have been installed in Whitehall, to supply information to the war bunker deep under the ministry of defence, code-named PINDAR. The cream of of British intelligence information would be gathered and flashed to Whitehall along optical fibre links, giving the cabinet an information system without equal.

It was a doomed vision. TRAWLERMAN was seen to be heading for disaster almost as soon as construction began in 1992. One of the problems was that there was only a small hatch that could take equipment deep into PINDAR. Everything, including mainframe computers, had to be dismantled and rebuilt. Because of the high classification of the information it handled, its security facilities made it incompatible with the other computers to which it had to be linked.

By the end of 1994, the computers were operating to a specification so loose that it did not include a requirement that they do the job for which they were installed. They were tested, switched off, dismantled, taken out and written off, at a cost to the public of £33m.

No one took responsibility for the disaster. Nobody knew who was responsible for what. A national audit office report even withheld the names of the computer manufacturers. Other corners of British intelligence were equally disorganised. According to a classified intelligence report prepared in 1994, in Northern Ireland there were 37 intelligence computer systems in operation, virtually none of which was compatible with any other.

VENGEFUL tracks vehicles around the province, using data from checkpoints and a network of automatic number plate readers. MANNEQUIN tracks people. According to the classified report, "VENGEFUL and MANNEQUIN need to be integrated to ensure we derive maximum operational benefit from the information they hold. A single intelligence database... is considered the key to successful intelligence analysis in support of army and RUC counterterrorist operations." No one (except perhaps the victims of terrorism) suffered for this lack. Instead, Labour is prosecuting the journalist who revealed this information, ex-Sunday Times correspondent Tony Geraghty, together with one of his alleged sources.

Nothing is new about the scale of the huge government IT projects that go wrong. It happened all the way through the 1980s, when the ministry of defence presided over £5bn worth of computer disasters: the Nimrod early warning aircraft, the Foxhunter radar, the Stingray torpedo, the Bates artillery targeting systems and the Royal Navy's integrated command and control system. The frontline of Britain's air defences were being managed from Portakabins in Northumberland while

contractors struggled for years to get the military radar and air defence system to work.

The social security department attempted unsuccessfully for years to get automated, under an operational strategy eventually costing £700m, at 1980 prices. In the 1990s, project Pathway for automated benefit payments at post offices, remains well behind schedule, with each side blaming the other. More than 30 such government computer projects may now come under Commons scrutiny, including systems for national insurance recording, MoT tests, and the prison service.

Tales of government cockups have become so prevalent that the magazine Computer Weekly took to nominating an annual award for the most significant new disaster to come to light. By 1998, competition for the award was so intense that a new category had to be created, reflecting outstanding achievements in fleecing the public at the same time as robbing them of services.

There was a sure winner: the £475m air traffic control centre at Swanwick. If it ever opens, it will be at least six years late and three times over cost. Some aspects of government conduct are hard to understand. At the home office immigration and nationality department, payments to Siemens are based on savings, so the more jobs go (and services decline), the greater the contractor's benefit. At Swanwick, US contractors Lockheed Martin were paid more than 90% of their fees at a stage when the system was years away from working.

Despite a string of Commons investigations, nothing changes. Only the public gets punished - first as taxpayers and second as consumers. The private sector is not without its share of megabuck problems, such as the Stock Exchange's Talisman project. But vast, global real time networks have been engineered and installed by banks and credit organisations with scarcely a hint of the problems that are epidemic in the British public sector.

Some cases reflect amateurism in the civil service, whereby standards applied elsewhere in industry or even in government are set aside. All too often, project planners think that their system is unique, and that they do not need to learn from elsewhere. When there is a disaster, senior officials get promoted and rewarded - not for achievement, but for silence. Companies that screw up get fresh contacts. The goal is to minimise whistleblowing, keep everyone on side, and keep the problem as far from view of MPs or the press as is possible. Private finance initiative projects have not remedied any of this, and may be going wrong faster than the others.

The best remedy is to ensure that when IT companies or officials are incompetent, their identities and errors are exposed to public view. Departments need to learn from mistakes. That means opening up the files not just to busy MPs but to the press and any taxpayer concerned about waste. This government was elected with a nifty plan to do just this. It's called freedom of information.

- Duncan Campbell is a freelance writer who specialises in computers.