More Naked Gun than Top Gun

The cream of US military intelligence last week had their bungled attempt to prosecute a bedroom hacker thrown out by a British court. Why are the spooks are firing blanks in the info-war?

By Duncan Campbell

***Guardian*, 26 November, 1997**

The three-year long case of the world's most notorious "information warfare" attack on US government computer systems collapsed last Friday. On a grey morning in a south London court, a 23-year-old computer programmer from Cardiff walked free as crown prosecutors told the judge it wasn't worth the cost of trying to hold his trial. They acknowledged that he had posed no threat to security.

But Matthew Bevan, who was obsessed with the X-Files and the search for alien spacecraft, and his 16-year-old accomplice, Richard Pryce, had achieved a notoriety out of all proportion to their actions. They were "Kuji" and "Datastream Cowboy" — hackers whose haphazard penetration of US Air Force and defence contractors' computers have been portrayed since 1994 as the work of foreign agents and the greatest electronic danger yet to hit the US Air Force on its home turf.

The collapse of Bevan's trial has exposed the US infowarriors. On the back of overblown rhetoric and oversold threats, they have won lavish funding from Congress for new military and intelligence "infowar" units, and recently sold their security services to private corporations.

But the inside story of the Bevan and Pryce cases shows their forensic work to have been so poor it would have been unlikely to have stood up in court and convicted

Bevan. The public portrayal of the two Britons as major threats to US national security was pure hype.

The case began in April 1994, when computer managers at an obscure US Air Force base at Rome, New York State, noticed that some of their computers had been penetrated via the Net. Over the next few weeks, a team of 50 infowar experts combed USAF and other computers to try to track the interlopers.

In May 1994, a USAF investigator told the Senate that the duo had “downloaded large volumes of data from penetrated systems”. But the computer used by Pryce to hack the US Air Force systems had already been discovered and seized by Scotland Yard. It was an aging 486 with a midget 170Mb hard disk. Bevan was no better equipped.

Although the two did allegedly download one or two classified files, those who have studied the detailed evidence in the case say that their approach was entirely haphazard and (so far as Bevan was concerned) motivated by the belief that a captured alien spacecraft, held secretly at the remote Nevada airbase Area 51 (as featured in last year’s film Independence Day), was reality.

In 1994, Bevan’s activities drew attention not in Nevada but Texas. Close to San Antonio is the Medina Annex of Lackland Air Force Base. Here, Air Force staff of the Consolidated Security Operations Center process communications from around the world. Like the real Area 51, Medina is one of the US government’s highest security facilities. San Antonio is home to the Electronic Security Command, the US Air Force section of the intelligence agency NSA. It also now hosts an Information Warfare Centre.

When on March 28, 1994 the emergency call came from New York to San Antonio, the infowar team were alerted to defend their country. Captain Kevin Ziese, chief of Advanced Counter Measures Research for the Infowar Centre, led a six-strong team whose members — or so he told Fortune magazine — “slept under their desks for three weeks, hacking backwards” until Pryce was arrested.

Since then, Ziese has hit the US lecture circuit and privatised his infowar business. As the WheelGroup corporation of San Antonio, he now sells “friendly” hacking services to top US corporations.

Meanwhile in Britain, the case against Bevan fell apart because testimony from Ziese and others wasn’t going to stand up in court. “Much of the US evidence would have collapsed on detailed scrutiny,” according to Peter Sommer, the LSE computer security and Internet expert who advised the defence teams for both men. Much of the “evidence” they gave to the Crown Prosecution Service was not valid evidence at all, but e-mails of edited files that had been relayed to Ziese and others.

Ziese’s technical investigation quickly ran dry, even after his team inserted their own anti-hacking and monitoring tools onto the Net. They had discovered that the hackers were entering USAF systems from two private Net sites, Cyberspace in Seattle and Mindvox in New York.

But where were the hackers really coming from? To answer that question, the USAF team obtained legitimate accounts on the Cyberspace computer. They used these to launch snooper programs codenamed Stethoscope and Pathfinder at the Cyberspace computer. It failed, as it could not determine how the hackers were phoning into Cyberspace.

US investigators have claimed the programs they used were legal because they did not access information that other users could not get. But they have refused to produce the programs.

Traditional police methods, not arcane infowar techniques, identified Pryce. A hacker who was an undercover informant had chatted to Pryce a few weeks earlier. Pryce had used his hacker name and given the informant his London phone number. Scotland Yard's Computer Crimes Unit were soon at Pryce's door with a search warrant. Bevan was eventually located in a similar way. His phone number was on Pryce's computer. Had it not been for Scotland Yard, the relatively innocuous Pryce and Bevan would never have been found — and the US Senate would still be hearing about "cyberterrorists" from faraway lands.

A further flaw in the USAF evidence appeared in May, when they refused to let defence experts examine and test programs they had used to monitor the Net. "Worst of all," says Sommer, "having set traps to catch hackers, they neglected to produce 'before' and 'after' file dumps of the target computers."

In the end, all the Americans handed over was patchy and circumstantial evidence that their computers had been hacked from Britain. To have attempted to fill in the holes in the evidence could have meant flying two dozen USAF witnesses to Britain to face lengthy and embarrassing cross-examination.

UK SPYMASTER SAYS TOO MANY SPOOKS SPOIL THE PLOT

British business security chiefs were last week lectured on the risks and realities of infowar at a conference on Business Crime and Risk at the Royal Society of Arts in London. But the highlight of the meeting was an unexpected call for British intelligence agencies to be cut down and realigned.

David Bickford was legal adviser to the intelligence and security services from 1987 until 1995, where he taught MI5 how to turn its work into evidence that its agents could present in court — skills that the US Air Force could do well to catch up with.

Bickford said that British intelligence “is not doing its job properly”. The £750 million a year cost of maintaining three intelligence agencies — the Security Service (MI5), Secret Intelligence Service (MI6) and GCHQ (responsible for electronic eavesdropping) — was now completely unjustified. There was “triplication of management, triplication of bureaucracy and triplication of turf battles”.

As a result, British intelligence was now turning “a blind eye to the fact that economic crime, including organised racketeering in narcotics, kidnap, extortion, product contamination and fraud, now poses the greatest threat to the security of the international community”.

Bickford revealed that, in 1995, the intelligence agencies had secretly suggested to the Major government that they develop links to large companies in order to provide them with “protective business intelligence”. The plan was turned down. Officially, it was claimed that the problem was distinguishing between “protective intelligence” and economic espionage. But the truth, he suggested, was that MI5, MI6 and GCHQ had bickered about how to finance and run the proposed new scheme.

Until difficulties like this were hammered out, said Bickford, taxpayers’ funds would be wasted and business damaged by the unavailability of important information that was kept only in government hands. A merger now would save “tens of millions of pounds”, and provide for the “focused direction, integration and analysis of electronic and human intelligence to reduce risk”, he added.

A cabinet office team is currently doing a year-long review of the structure of British intelligence. Their review should be “quite fierce”, suggested Bickford.

Internal threats had all but disappeared — and with them the raison d’etre of MI5. The main threat to Britain now was “serious economic crime” and “super-terrorism”, involving the use of weapons of mass destruction, he said. Because of “the common international nature of these threats”, arguments for having three different intelligence services “falls at the first hurdle”.

Not only were “operational officers with long experience in intelligence” being lost to the private sector, others were lost because they had to take up management posts instead of carrying on in intelligence. Tax payers were having to pay for this “waste of experience”, Bickford claimed.

A new “national intelligence agency” should be formed, he added, in order to provide protective business intelligence. It could even charge for its services. It was “long overdue” for the Parliamentary Intelligence Oversight Committee to instigate the process of amalgamating the three agencies.

Hostility and in-fighting between MI5 and MI6 has long been notorious. The situation only began to change in the mid-1970s, when the two agencies formed a joint section to fight Irish terrorism. Since 1990, MI5 has seen its traditional concerns of Soviet espionage and so-called “internal subversion” all but vanish. Faced with the additional threat of a ceasefire in Ireland, MI5 has sought to move into police areas including fraud, money laundering, narcotics and organised crime. MI6 and GCHQ have also been retargeted into these areas.

Bickford's call for more intelligence and security expertise for business was backed by Sir Peter Imbert, former Commissioner of the Metropolitan Police, and other senior ex-police officers.

While legal adviser to MI5 and MI6, Bickford helped draft the legislation that brought the once officially invisible organisations "in from the cold" and put them on a statutory legal basis. Since leaving the agencies, Bickford has attacked the government's willingness to allow British offshore islands to remain as tax havens, claiming that this constituted tacit support for money laundering and organised crime.