

Schoolboy hacker

Adapted from an article in *The Guardian*, 22 March 1997, by Christopher Elliot

A SIXTEEN-YEAR-OLD schoolboy using a cheap computer sparked an "international hunt" for an Eastern European spy ring, a court heard yesterday. Richard Pryce, a music student, had hacked into military computers in the US from his bedroom on at least 200 occasions before he was arrested, said Simon Dawson, prosecuting at Bow Street magistrates court yesterday.

"He had a predilection for missile and artificial intelligence sites. It caused enormous consternation to the American authorities," Mr Dawson said.

Pryce pleaded guilty to 12 charges of gaining unauthorised access to computers and was fined £1,200. Mr Dawson said: "The substantial volume of military files that had been downloaded from the US military would have covered 2,000 to 3,000 A4 pages." The US authorities claimed a number of the files were sensitive.

The hunt for Pryce, now 19, began against a background of increasing concern by the US military, particularly the air force, that their computer security was being regularly breached by hackers.

The US Office of Special Investigations had identified several individuals by their hacking soubriquets and were now looking for the Datastream Kid - whose real identity was Pryce.

Pryce, who was taking A levels in computer studies and music, had been given a £750 computer to help him. He had become interested in hacking through the bulletin boards on the Internet which swap techniques, codes and passwords.

To help him he had acquired a piece of software known as a bluebox, which replicates a series of dial tones which play to the 0800

freephone numbers through old exchanges. The bluebox fools the exchange into opening a free phone number. Pryce got his free phone via an exchange in Bogota.

"This left him secure in the knowledge that his parents would not receive the telephone bill for all the telephone usage," Mr Dawson said.

The second stage was to find the necessary codes to get him into the restricted computer sites.

These may be passed around on the hacker's bulletin board or the hacker may introduce a computer programme colloquially known as a "sniffer" which captures a whole range of data from the authorised user of the restricted system.

Within it the hacker hopes there is a password. He then runs the captured information through a decryption programme to find the solution to access of the site.

Using these techniques Pryce got into the Griffiss air base and the Lockheed Space and Missile company in California.

Pryce was arrested by Scotland Yard officers after weeks of surveillance and the logging of calls following a tip from US officials.

"He became immersed in the game and it was one way of making friends, friends he never met, whose real names he never knew. He meant no harm, made no material gain and the last thing he was thinking of was subverting the western alliance," Mr Geoffrey Robertson QC said.

Pryce had been offered £30,000 by a tabloid newspaper for his story, film and book rights but had turned them all down. He wanted to pursue his career as a musician.

© *The Guardian*